

Register your instrument!
www.eppendorf.com/myeppendorf

epBlue GxP™

Software-Bedienungsanleitung

Software-Version 40.2

epMotion VAC sealing foil U.S. Pat. No. 6,666,978

epMotion optical sensor U.S. Pat. No. 6,819,437

epMotion gripping tool U.S. Pat. No. 7,462,327

The software of the device (firmware) contains open source software. License information is available on request from Eppendorf AG.

Only for epMotion M5073, M5073c, 5075m and 5075mc: Limited Use Label License NOTICE TO PURCHASER; LIMITED LICENSE FOR RESEARCH USE ONLY.

This product and its use may be covered by one or more patents owned by Gen-Probe Incorporated. The purchase price for this product includes only limited, nontransferable rights under certain claims of certain patents owned by Gen-Probe Incorporated to use this product for research purposes only. No other rights are conveyed. Purchaser is not granted any rights under patents of Gen-Probe Incorporated to use this product for any commercial use. Further information regarding purchasing a license under patents of Gen-Probe Incorporated to use this product for any other purposes, including, without limitation, for commercial use, may be obtained by contacting Gen-Probe Incorporated, Attn: Business Development Department, 10210 Genetic Center Drive, San Diego, California 92121-4362, U.S.A.

5075 901.269-00/042013

Inhaltsverzeichnis

1 Anwendungshinweise

1.1 Anwendung dieser Anleitung

Die Bedienungsanleitung Ihrer epMotion besteht aus einer Anleitung zur Hardware und einer Anleitung zur Software. Für optionale Software-Module existieren separate Anleitungen.

Die Bedienungsanleitung ist Teil des Produkts.
Die aktuelle Version der Bedienungsanleitung finden Sie auf unserer Internetseite www.eppendorf.com.

- Lesen Sie die Bedienungsanleitung vollständig, bevor Sie die das Gerät verwenden.
- Bewahren Sie die Bedienungsanleitung gut erreichbar auf.
- Geben Sie das Gerät nur mit Bedienungsanleitung weiter.
- Wenn die Bedienungsanleitung verloren gegangen ist, ersetzen Sie diese sofort. Wenden Sie sich dazu an die Eppendorf AG.

1.2 Gefahrensymbole und Gefahrenstufen

Die Sicherheitshinweise in dieser Anleitung haben die folgenden Gefahrensymbole und Gefahrenstufen:

1.2.1 Gefahrensymbole

	Sachschaden	

1.2.2 Gefahrenstufen

GEFAHR	*Wird* zu schweren Verletzungen oder zum Tod führen.
WARNUNG	*Kann* zu schweren Verletzungen oder zum Tod führen.
VORSICHT	Kann zu leichten bis mittelschweren Verletzungen führen.
ACHTUNG	Kann zu Sachschäden führen.

1.3 Darstellungskonventionen

Darstellung	**Bedeutung**
1. 2.	Handlungen in vorgegebener Reihenfolge
▸	Handlungen ohne vorgegebene Reihenfolge
•	Liste
Text	Display-Text oder Software-Text
ⓘ	Zusätzliche Informationen

1.4 Abkürzungen

BCR
Barcode Reader

CSV
Comma Separated Value

CFR
Code of Federal Regulation (Bundesgesetz der USA)

DNA
Deoxyribonucleic acid – Desoxyribonukleinsäure (DNS)

DWP
Deepwell-Platte

epT.I.P.S.
eppendorf **T**otally **I**ntegrated **P**ipetting **S**ystem

HEPA
High Efficiency Particulate Air (Filter)

GxP
Good Practice — Richtlinien für gute Arbeitspraxis

IQ
Installation Qualification

LH
Liquid Handling

LIMS
Labor-Informations- und Management-System

MTP
Mikrotestplatte

OQ
Operational Qualification

PCR
Polymerase-Kettenreaktion

PDF
Portable Document Format

TMX
ThermoMixer

USB
Universal Serial Bus

UV
Ultraviolette Strahlung

VAC
Vakuumeinheit

1.5 Glossar

A

Administrator
Anwender, der Rechte besitzt, um epBlue zu verwalten.

Administrator Lab
Anwender, der Rechte besitzt, um Applikationen und Labware zu verwalten.

Applikation
Programm für eine bestimmte Anwendung. Zu einer Applikation gehören die Prozedur und die Bestückung des Worktable.

Arbeitsvolumen
Volumen einer Labware. Die epMotion befüllt ein Gefäß bis zum Arbeitsvolumen. Das Arbeitsvolumen ist kleiner als das Füllvolumen.

Audit Trail
Chronologische Aufzeichnung von Ereignissen, die den Datenbestand oder den Zustand des Systems verändern.

B

Barcode Reader
Gerät, um einen Barcode zu scannen.

Befehl
Schritt in einer Prozedur. Für Befehle können unterschiedliche Parameter eingestellt werden. Jeder Befehl löst eine Aktion aus, z. B. den Transport von Flüssigkeit.

C

CleanCap
Optionale Ausstattung der epMotion. Zum CleanCap gehören HEPA-Filter und mindestens eine UV-Lampe.

CSV-Datei
Textdatei zum Austauschen strukturierter Informationen.

D

Dosierwerkzeug
Werkzeug, das Flüssigkeiten aufnimmt und abgibt. Verfügbar sind Einkanal-Dosierwerkzeuge und Achtkanal-Dosierwerkzeuge für unterschiedliche Volumenbereiche.

E

Entry-Liste
ID-Liste, die beim Start der Applikation einer Labware zugewiesen wird. Die ID-Liste enthält den Namen der Labware, IDs für die Positionen der Labware und Beschreibungen. epBlue importiert und exportiert die IDs der Labware mit Hilfe von Entry-Listen. epBlue verarbeitet Entry-Listen in den Formaten CSV und XML.

epBlue
Software, um Applikationen und Labware zu erstellen und zu verwalten. Mit der Software wird die epMotion gesteuert. Die Software enthält eine Benutzerverwaltung. epBlue ist modular erweiterbar.

epBlue GxP
Das Modul epBlue GxP ermöglicht eine elektronische Dokumentation gemäß dem Bundesgesetz 21 CFR Part 11 der Vereinigten Staaten von Amerika.

epBlue ID
Das Modul epBlue ID ermöglicht die Verfolgung von Proben während der Applikation. Dazu wird die Labware mit IDs gekennzeichnet. Die Verfolgung der Proben wird automatisch dokumentiert.

epT.I.P.S. Motion
Pipettenspitzen der epMotion. Auf der epMotion können nur epT.I.P.S.® Motion verwendet werden. epT.I.P.S.® Motion sind mit und ohne Filter erhältlich.

F

Füllvolumen
Maximales Volumen einer Labware. Bis zum Füllvolumen entnimmt die epMotion Flüssigkeit aus der Labware. Das Füllvolumen ist höher als das Arbeitsvolumen.

G

Gefäß
Reaktionsgefäß oder einzelnes Well einer Platte.

Greifer
Werkzeug, dass Labware transportiert.

H

HEPA-Filter
Luftfilter. Der Luftfilter verhindert, dass Partikel wie Staub und Keime aus der Umgebung in den Arbeitsraum der epMotion gelangen.

Höhenadapter
Adapter, für niedrige Labware. Um Wege des Werkzeughalters zu verringern und damit die Laufzeit der Applikation zu verkürzen, werden die Höhenunterschiede zwischen der Labware ausgeglichen.

I

ID
Zeichenfolge, mit der das Modul epBlue ID die Labware identifiziert.

Input-Liste
ID-Liste mit Informationen über Quell-Labware. Die Input-Liste enthält die IDs der Quellpositionen. epBlue erstellt eine Input-Liste für jede Quell-Labware, deren ID-Verfolgung aktiviert ist.

L

Labware
Racks, Platten, Spitzen usw., die auf dem Worktable platziert werden.

M

MagSep
System aus Magnetfingermodul, ThermoMixer, PrepRack und Reagenzien zur Nukleinsäure-Präparation mit der epMotion.

MultiCon PC
Eppendorf MultiCon™ PC. Über den Computer steuern Sie mit der Software epBlue Ihre epMotion.

P

Pattern
Muster, in dem Flüssigkeit aufgenommen und abgegeben wird. Pattern werden in einem Transferbefehl festgelegt. Pattern werden definiert als Reguläre Pattern und Irreguläre Pattern. Pattern sind in x- und y-Richtung unabhängig.

Platz
Bereich auf dem Worktable, auf dem Labware platziert wird.

Prozedur
Folge von Befehlen, die nacheinander ausgeführt werden. Teil einer Applikation.

Q

Quell-Labware
Rack oder Platte mit Quell-Positionen.

Quell-Position
Position in der Labware, aus der während der Applikation Flüssigkeit ausschließlich entnommen wird.

R

Rack
Halter für Gefäße oder Pipettenspitzen.

Reservoir
Reservoirs dienen zur Vorlage von Reagenzien. Reservoirs werden in ein ReservoirRack gehängt oder direkt auf dem Worktable platziert.

Restvolumen
Volumen, das aus einem Gefäß nicht entnommen werden kann. Der in der Software definierte Abstand der Pipettenspitze zum Gefäßboden und die definierte Eintauchtiefe der Pipettenspitze in die Flüssigkeit müssen eingehalten werden. Deshalb kann die Pipettenspitze das Volumen nicht aufnehmen. Das Restvolumen ist abhängig von der Gefäßgeometrie.

Result-Liste
ID-Liste mit Informationen über Ziel-Labware und Zwischen-Labware. Die Result-Liste enthält die IDs von Zielpositionen und Zwischenpositionen. epBlue erstellt eine Result-Liste für jede Ziel-Labware und Zwischen-Labware, deren ID-Verfolgung aktiviert ist.

S

SafeRack
Rack mit ep.T.I.P.S. Motion Pipettenspitzen. Das SafeRack besitzt eine Unterteilung, welche die Kontamination benachbarter Spitzen verhindert. Wenn sie Spitzen mehrfach verwenden möchten, benutzen Sie SafeRacks.

Signatur, digitale
Technischer Begriff für eine elektronische Signatur, die mittels kryptografischer Verfahren ausgeübt wird.

Signatur, elektronische
Rechtlicher Begriff für ein elektronisches Äquivalent einer rechtlich bindenden handschriftlichen Unterschrift. Die rechtliche Bedeutung verschiedener Formen von elektronischen Signaturen ist in länderspezifischen Gesetzen definiert.

T

Thermoadapter
Wärmeleitender Adapter, der Platten aufnimmt.

Thermoblock
Thermoadapter, der fest mit einer PCR-Platte oder einem PCR-Gefäß verbunden ist.

Thermomodul
Wärmeplatte für Labware. Die Wärmeplatte ist im Worktable integriert.

Thermorack
Temperierbares Rack für kleinere Gefäße, z. B. Safe-Lock-Reaktionsgefäße für 0,5 mL, 1,5 mL oder 2 mL.

Ü

Überhub
Bewegung des Kolbens. Die Flüssigkeit in der Pipettenspitze wird nach dem Pipettierschritt abgegeben.

V

Vakuumeinheit
Die Vakuumeinheit saugt durch Unterdruck Flüssigkeit aus einer Filterplatte. Die Vakuumeinheit besteht aus Vakuumkammer, Vakuumpumpe und Vakuumrahmen.

W

Worktable
Arbeitsfläche der epMotion, auf der Labware und Werkzeuge platziert werden. Der epMotion-Worktable wird in der Software als epBlue-Worktable dargestellt.

Z

Zertifikat, digitales
Datensatz, der es ermöglicht, einer digitalen Signatur die Identität einer Person, einer Organisation oder eines Systems zuzuordnen.

Ziel-Labware
Rack oder Platte mit Zielpositionen.

Ziel-Position
Labware, in die während der Applikation Flüssigkeit ausschließlich hinein gegeben wird

Zwischen-Labware
Rack oder Platte mit Zwischenpositionen.

Zwischen-Position
Position in der Labware, die sowohl Quelle als auch Ziel von Flüssigkeitstransfers ist.

1.6 Änderungshistorie

Bedienungsanleitung	Version	Datum	Software-Version	Änderungen
5075 901.269	00	März 2014	epBlue 40.2	Neuerstellung der Anleitung

2 Produktbeschreibung

2.1 Produkteigenschaften

2.1.1 epBlue GxP

Die Software epBlue GxP unterstützt den Anwender beim Erzeugen und Verwalten elektronischer Dokumentation. Die Software wurde entsprechend den Bestimmungen des Bundesgesetzes 21 CFR Part 11 der USA entwickelt.

epBlue GxP besitzt folgende Funktionen:
- Autorisierungsschema für Applikationen und Protokolle festlegen.
- Applikationen und Revisionen verwalten.
- Anwenderdaten als digital signierte PDF-Dokumente exportieren und archivieren.
- Benutzerkonten verwalten.
- Audit Trail automatisch und kontinuierlich aufzeichnen.
- Prüfsummen kontrollieren.
- Komponenten von Hardware und Software verifizieren.
- Optional epBlue ID: Labware, die mit einem Barcode markiert ist, durch ID-Listen verfolgen.

Sie können die Entwicklungs- und Änderungsdokumentationen für epMotion 5075 mit epBlue GxP bei der Eppendorf AG einsehen.

2.1.2 epMotion 5075 mit epBlue GxP

Sie können die epMotion 5075 mit MultiCon PC zusammen mit der installierten Software epBlue GxP bestellen.
Das System wird von Eppendorf validiert und dokumentiert ausgeliefert. Das System wird beim Kunden aufgestellt.

2.1.3 Umrüstsatz für epBlue GxP

Sie können die Software epBlue GxP als Umrüstsatz zu einer epMotion 5075 mit MultiCon PC bestellen.

Der Umrüstsatz enthält keine gerätespezifische Dokumentation, z. B. Protokolle. Der Anwender ist für die Validierung des Systems verantwortlich.



Um Ihr Gerät warten und zertifizieren zu lassen, stehen Ihnen die Serviceleistungen der Eppendorf AG zur Verfügung.
Informationen über die Servicedienstleistungen erhalten Sie auf unserer Internetseite www.eppendorf.com.

2.1.4 epBlue ID

Sie können die Software epBlue GxP mit dem Modul epBlue ID erweitern.
Informationen zu epBlue ID finden Sie in der Software-Bedienungsanleitung.

2.1.5 epBlue-Assistants

Sie können in epBlue GxP mit den epBlue-Assistants Applikationen erstellen. Um die Vorgaben von GxP zu erfüllen, werden die Applikationen nicht innerhalb der epBlue-Assistants ausgeführt.



- Applikationen von epBlue-Assistants mit der Funktion *Save as* speichern.
- Applikationen im *Application Editor* von epBlue starten.

Mit epBlue-Assistants erstellte Applikationen haben den Status *unsigned*.

2.2 Lieferumfang

Anzahl	Beschreibung
1	**Software epBlue GxP**
1	**Installationsanleitung epBlue GxP**
1	**Bedienungsanleitung epBlue GxP**
1	**Dokumentationsordner** Ordner für Zertifikate und Dokumentationen

Informationen zum Lieferumfang des Gerätes und der Software epBlue GxP finden Sie auf dem Lieferschein.

3 Allgemeine Sicherheitshinweise

Für die Verwendung der epMotion mit der Software epBlue GxP gelten bestimmungsgemäßer Gebrauch und Sicherheitshinweise aus der Hardware-Bedienungsanleitung und der Software-Bedienungsanleitung.



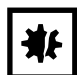
ACHTUNG! Datenverlust durch Stromausfall.
Wenn die Stromversorgung ausfällt, wird der Computer unerwartet ausgeschaltet. Daten können nicht mehr in die epBlue-Datenbank geschrieben werden. Die epBlue-Datenbank wird unvollständig.

- Schließen Sie den Computer an eine unterbrechungsfreie Stromversorgung an.



ACHTUNG! Datenverlust durch Manipulation.
Manipulationen an den Einstellungen des Betriebssystems und an den Einstellungen von Software und Hardware beeinträchtigen den fehlerfreien Betrieb.
Die Aufzeichnung elektronischer Dokumente kann gestört werden. Die Kommunikation zwischen epMotion und epBlue kann gestört werden.

- Verändern Sie die Systemkonfiguration im Betriebssystem nicht, z. B. Treiber.
- Das Betriebssystem darf nur vom autorisierten Service verändert werden.



ACHTUNG! Löschen von Daten aus der Datenbank beim Archivieren.
Wenn Sie Daten archivieren, exportiert epBlue die Daten als PDF-Dokumente. Die Daten werden aus der epBlue-Datenbank entfernt.
Archivierten Daten können nicht wieder in die epBlue-Datenbank importiert werden.

- Archivieren Sie keine Daten, die Sie noch benötigen.

4 Arbeiten gemäß gesetzlicher Bestimmungen

epBlue GxP stellt Ihnen Funktionen bereit, die Sie bei der Erstellung und Bereitstellung elektronischer Dokumente unterstützen. Um weitere gesetzliche Anforderungen zur Anerkennung Ihrer elektronischen Dokumente bei Behörden zu erfüllen, müssen Sie als Betreiber des Systems epMotion 5075 mit epBlue GxP besondere Rahmenbedingungen schaffen und einhalten. Diese sind für das US-amerikanische Bundesgesetz 21 CFR Part 11 für Einreichungen bei der US Food and Drug Administration im Folgenden exemplarisch zusammengestellt. Gesetzliche Anforderungen für andere Behörden und in anderen Ländern können davon abweichen.

Verpflichtung zur Anwenderschulung	§11.10 (i). Personen, die epBlue GxP pflegen und nutzen, müssen eine geeignete Ausbildung, Erfahrung und Schulung aufweisen. Entsprechende Schulungen werden von Eppendorf angeboten.
Verbindlichkeit der digitalen Signatur	§11.10 (j). Sie sind verpflichtet, schriftlich festgelegte Regeln für den Umgang mit digitalen Signaturen in epBlue GxP und deren rechtliche Bindung zu etablieren und einzuhalten. Es wird empfohlen, die Verpflichtung zur Einhaltung dieser Regeln von jedem Benutzer mit einer handschriftlichen Unterschrift bestätigen zu lassen. §11.50 (a). Sie sind verpflichtet, die Identität der zur Ausübung digitaler Signaturen berechtigten Personen zu prüfen. Es wird empfohlen, die Identitätsprüfung schriftlich zu dokumentieren und den echten Vor- und Nachnamen beim Anlegen eines Benutzerkontos in epBlue GxP einzugeben. Diese Angaben erscheinen in den elektronischen Dokumenenten. §11.100 (c) Personen, die elektronische Signaturen verwenden, sollen vor oder zur Zeit ihrer Benutzung der Behörde (FDA) bescheinigen, dass die elektronischen Unterschriften in ihrem System, die am oder nach dem 20. August 1997 benutzt wurden, als rechtlich verbindliches Äquivalent zu herkömmlich handgeschriebenen Unterschriften gelten.
Umgang mit Systemzugängen	§11.200 (a)(3). Sie müssen sicherstellen, dass eine elektronische Signatur nicht von einer anderen Einzelperson als dem rechtmäßigen Eigentümer des Systemzugangs ausgeübt werden kann. Bei Verlust von Passwörtern kann ein Benutzer der Benutzergruppe *Administrator* einem Benutzer ein neues Passwort zuweisen. Eppendorf empfiehlt schriftlich festzulegen, dass bei Änderung eines Passworts durch einen Benutzer der Benutzergruppe *Administrator* der betreffende Benutzer anwesend sein muss und sofort ein nur ihm bekanntes Passwort für sein Benutzerkonto festlegen muss.

Verfügbarkeit elektronischer Dokumente	§11.10 (c). Sie sind verpflichtet, den ordnungsgemäßen Zugriff auf die Dokumente während der Aufbewahrungsfrist zu gewährleisten. In epBlue GxP stehen Ihnen dazu die Funktionen Backup und Archivierung zur Verfügung. Um Datenverlust durch Stromausfall zu vermeiden, müssen Sie das System an einer unterbrechungsfreien Stromversorgung betreiben. §11.300 (c). Sie sind verpflichtet, Verfahren bei Verlust oder Diebstahl von Systemzugangsdaten zu etablieren und zu befolgen. Um Systemzugänge in epBlue GxP zu verwalten, müssen Sie ein Benutzerkonto der Benutzergruppe *Administrator* haben. Das System kann nicht ohne Neuinstallation administriert werden, wenn kein gültiger Administrator-Zugang vorhanden ist (z.B infolge von Passwortverlust oder automatischer Sperrung nach mehrmaliger Fehleingabe des Passworts). Sie sind für die Gewährleistung des Administrator-Zugangs verantwortlich. Eppendorf empfiehlt, mindestens einen zweiten Administrator-Zugang in epBlue GxP einzurichten.
Umgang mit der Systemdokumentation	§11.10 (k). Sie sind verpflichtet, eine Regelung über die Verteilung, den Zugang und die Benutzung der Dokumentationen für den Betrieb und die Pflege von epBlue GxP und der epMotion 5075 zu etablieren und einzuhalten.
Systemwartung	§11.10 (h) und §11.300 (e). Sie sind verpflichtet, die ordnungsgemäße und sichere Funktion der Systemkomponenten zu gewährleisten und sicherzustellen, dass keine unbefugten Änderungen am System vorgenommen wurden. Hierzu bietet Eppendorf Wartungsverträge an.

Die Paragraphen beziehen sich auf 21 CFR Part 11. Sie finden den Gesetztestext im Internet http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm.

5 Grundlegende Konzepte

In diesem Kapitel erfahren Sie, wie elektronische Dokumente in epBlue GxP erzeugt und verwaltet werden.

5.1 Benutzergruppen und deren Rechte

Beim Arbeiten mit Elektronischen Dokumenten müssen sämtliche Manipulationen jederzeit und eindeutig einer Person zugeordnet werden. epBlue GxP stellt dies sicher. epBlue GxP speichert die Signatur des Anwenders, der ein elektronisches Dokument verändert, im Audit Trail und bei der Erstellung einer digitalen Signatur.

Um die Anwender zu verwalten, besitzt epBlue GxP 5 Benutzergruppen. Mit den Benutzergruppen können Sie die Rechte von Anwendern entsprechend deren Rollen in Ihrer Organisation festlegen. Jede Benutzergruppe besitzt spezielle Rechte zu Ausführung von digitaler Signaturen.

Benutzergruppe	Beispiel für Rechte der Benutzergruppen
Guest	Labormitarbeiter, der freigegebene Applikationen ausführt, aber keine Applikationen erstellt.
User Level 1	Labormitarbeiter, der elektronische Dokumente erstellt ("create") und freigegebene Applikationen ausführt.
User Level 2	Labormitarbeiter, der für die Prüfung und Validierung ("review") elektronischer Dokumente verantwortlich ist.
Administrator Lab	Labormanager, der für die Freigabe ("authorize") und das Austauschen elektronischer Dokumente verantwortlich ist, sowie Benutzerkonten und Daten verwaltet.
Administrator	Administrator des Systems, der Gerät und Software pflegt, die epBlue-Datenbank sichert und das Systems verwaltet. Der Administrator erstellt keine Applikationen und führt keine Applikationen aus.

Eine detaillierte Beschreibung der Benutzergruppen und ihrer Rechte finden Sie innerhalb der Software epBlue GxP.

Die Rechte der Benutzergruppen *Guest*, *User Level 1*, *User Level 2* und *Administrator Lab* bauen aufeinander auf.

5.1.1 Schutz vor unbefugtem Zugriff

epBlue GxP sichert den Zugang zu epBlue GxP durch folgende Funktionen:
- epBlue GxP-Fenster sperren, wenn der angemeldete Anwender eine definierte Zeit keine Aktivitäten vorgenommen hat.
- Benutzerkonten sperren, wenn das Passwort mehrfach falsch eingegeben wurde.
- Optional: Gültigkeit von Benutzerkonten zeitlich einschränken, siehe Software-Bedienungsanleitung.
- Optional: Gültigkeit von Passwörtern zeitlich einschränken.
- Komplexe Regeln für Passwörter.

5.1.2 Regeln für Passwörter

Für Passwörter gelten folgende Regeln:
- Länge mindestens sechs Zeichen.
- Mindestens ein Großbuchstabe.
- Mindestens ein Kleinbuchstabe.
- Mindestens eine Ziffer.
- Mindestens ein Sonderzeichen.

5.2 Elektronische Dokumente

Elektronische Dokumente sind Daten, die eine digitale Signatur besitzen.

Folgende Daten können als Elektronische Dokumente gespeichert werden:
- Applikationen
- Protokolle von Applikationen mit dem Status *authorized*

epBlue GxP speichert Elektronische Dokumente und Signaturen in der epBlue-Datenbank. Elektronische Dokumente können nicht aus epBlue GxP gelöscht werden. Elektronische Dokumente können archiviert werden.

5.2.1 Digitale Signaturen

epBlue GxP erzeugt digitale Signaturen nach dem standardisierten Verfahren Digital Signature Algorithm (DSA).

Wenn Elektronische Dokumente verwendet werden, prüft epBlue GxP, ob die Signaturen gültig sind. Wenn ein signiertes Dokument verändert wurde, wird dessen Signatur ungültig. epBlue GxP zeigt eine Fehlermeldung.

Um ein Dokument zu signieren, müssen Sie Ihren Namen und Ihr Passwort eingeben.

5.2.2 Status von Elektronischen Dokumenten

Jede Signatur besitzt eine Bedeutung (*Meaning*).

Der Status eines Elektronischen Dokuments hängt von Status und Zahl der vergebenen Signaturen ab. Ein Elektronisches Dokument besitzt maximal 3 Signaturen mit unterschiedlichem Status und kann von maximal 3 Anwendern signiert werden.

Tab. 5-1: Status Elektronischer Dokumente

Status:	unsigned	created	reviewed	authorized
Zahl der Signaturen	keine	1	2	1, 2 oder 3
Bedeutung für Applikationen	Jedes neu angelegte Dokument besitzt den Status *unsigned*.	Der Signierende bestätigt, dass er die Applikation erstellt und getestet hat.	Der Signierende bestätigt, dass er die Applikation geprüft hat.	Der Signierende autorisiert die Applikation für die Verwendung.
Bedeutung für Protokolle		Der Signierende bestätigt, dass er den Lauf vorschriftsgemäß ausgeführt hat.	Der Signierende bestätigt, dass er den Lauf vorschriftsgemäßen geprüft hat.	Der Signierende autorisiert das Protokoll und damit den Lauf. Damit gibt er z. B. bearbeitete Proben frei.

Der *Administrator* legt Zahl und Status der Signaturen fest, für die Freigabe eines Dokuments benötigt werden. Zahl und Status der Signaturen werden separat für Applikationen und Protokolle festgelegt.

epBlue GxP erzwingt das "Mehraugenprinzip". Ein Dokument kann von einem Anwender nur ein Mal signiert werden.

Ob ein Anwender berechtigt ist, Signaturen eines bestimmten Status zu vergeben, hängt von seiner Benutzergruppe ab.

5.2.3 Revisionen

epBlue GxP verwaltet die Revisionen von signierten Applikationen automatisch. Damit dokumentiert epBlue GxP die Entwicklung der Applikationen.

- Der Status einer Applikation bezieht sich auf eine Revision.
- Revisionen einer Applikation können unterschiedliche Status aufweisen.
- Wenn Sie eine signierte Applikation ändern und speichern, legt epBlue GxP eine neue, nicht signierte Revision an.
- Ältere Revisionen können gelesen werden, aber nicht verändert werden.
- Revisionen können ausgeführt werden, bis eine neuere Revision als *authorized* signiert wird.
- Für jede Revision werden Protokolle aufgezeichnet.

5.2.4 Umgang mit signierten Applikationen

Eine Applikation ist signiert, wenn die aktuelle Revision eine Signatur besitzt.

Tab. 5-2: Für signierte Applikationen gelten folgende Einschränkungen:

Editieren	• Wenn Sie die Applikation editieren und speichern, legt epBlue GxP eine neue Revision an. • Um dies zu vermeiden, können Sie die geänderte Applikation unter einem neuen Namen abspeichern. • Die Eigenschaften einer signierten Applikation können nicht verändert werden.
Labware	• epBlue GxP speichert eine Kopie der verwendeten Labware zusammen mit der signierten Applikation. • Damit wird gesichert, dass signierte Applikationen ausgeführt werden können, wenn die Labware-Bibliothek verändert wurde. • Eine signierte Applikation wird immer mit der Labware durchgeführt, die in der Applikation gespeichert ist.
Ausführen	• Wenn eine Applikation ausgeführt wird, kann der Anwender die voreingestellten *Levelsensor Options* nicht ändern.
Verwaltung	• Die Applikation kann nicht gelöscht werden. Um die Applikation aus dem System zu entfernen, müssen Sie diese archivieren. • Die Funktion *Cut* steht nicht zur Verfügung. • Wenn Sie die Applikation kopieren, werden die Signaturen nicht mit kopiert. Signieren Sie die Applikationen nach dem Kopieren. • Wenn Sie die Applikation exportieren, werden die Signaturen nicht mit exportiert. • Ordner, die signierte Applikationen enthalten, können nicht gelöscht oder umbenannt werden. • Benutzerkonten, unter denen signierte Applikationen gespeichert sind, können nicht gelöscht werden.

5.2.5 Digitales Schlüsselpaar

Wenn ein neues Benutzerkonto angelegt wird, berechnet epBlue GxP ein individuelles digitales Schlüsselpaar und speichert es in der epBlue-Datenbank. Das digitale Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel.

Der private Schlüssel ist mit dem Passwort des Benutzerkontos geschützt. Der private Schlüssel wird benutzt, um digitale Signaturen zu erzeugen.

Mit dem öffentlichen Schlüssel werden digitale Signaturen von Dokumenten geprüft. Die Dokumente können sich in der epBlue-Datenbank befinden und als PDF-Dokument vorliegen.

5.2.6 Zertifikate

Mit einer Systemsignatur kann nachgewiesen werden, dass ein PDF-Dokument von epBlue GxP erzeugt wurde (Authentizität) und nach dem Exportieren nicht verändert wurde.

Die Systemsignatur gilt für ein epBlue-System. Die Systemsignatur ist für alle PDF-Dokumente identisch, die von diesem epBlue-System stammen.

Sobald ein elektronisches Dokument in epBlue GxP geöffnet wird, wird die digitale Signatur überprüft. Um die Gültigkeit der Signaturen in PDF-Dokumenten zu prüfen, exportieren Sie die öffentlichen Schlüssel zusammen mit den Informationen über den Anwender als PKCS#7 Zertifikate (.cer-Dateien) aus epBlue.

Mit exportierten Zertifikaten können Sie erzeugte PDF-Dokumenten und darin enthaltenen Signaturen prüfen.

Tab. 5-3: Prüfungen von PDF-Dokumenten und darin enthaltenen Signaturen

Zertifikat	Beschreibung
Benutzerzertifikat	Gültigkeit der digitalen Signatur des Anwenders prüfen, der das Dokument aus epBlue GxP exportiert hat. Nachweis, dass das Dokument von einer bestimmten Person exportiert nicht verfälscht wurde.
Systemzertifikat	Gültigkeit der digitalen Signatur des epBlue-Systems prüfen, mit dem das Dokument erzeugt wurde. Nachweis, dass das Dokument mit einem bestimmten epBlue-System exportiert wurde.
Master-Zertifikat	Gültigkeit der Benutzerzertifikate und Systemzertifikate prüfen, mit denen das Dokument überprüft wird. Nachweis, dass die digitalen Signaturen von epBlue GxP erzeugt wurden. Das Master-Zertifikat ist das Stammzertifikat der Systemzertifikate und der Benutzerzertifikate.

5.3 Audit Trail

Der Audit Trail wird chronologisch aufgezeichnet.

In einem Audit Trail werden folgende Informationen gespeichert:
- Änderung von Applikationen und Labware
- Signatur von Daten
- Ausführung, Unterbrechung und Abbruch von Applikationen
- Zustand und Änderungen der Systemkonfiguration
- Anmeldung und Abmeldung der Anwender
- Änderung von Benutzerkonten

Der Audit Trail ist Teil der Dokumentation. Der Audit Trail kann als signiertes PDF-Dokument exportiert werden.

5.3.1 Aktionen begründen

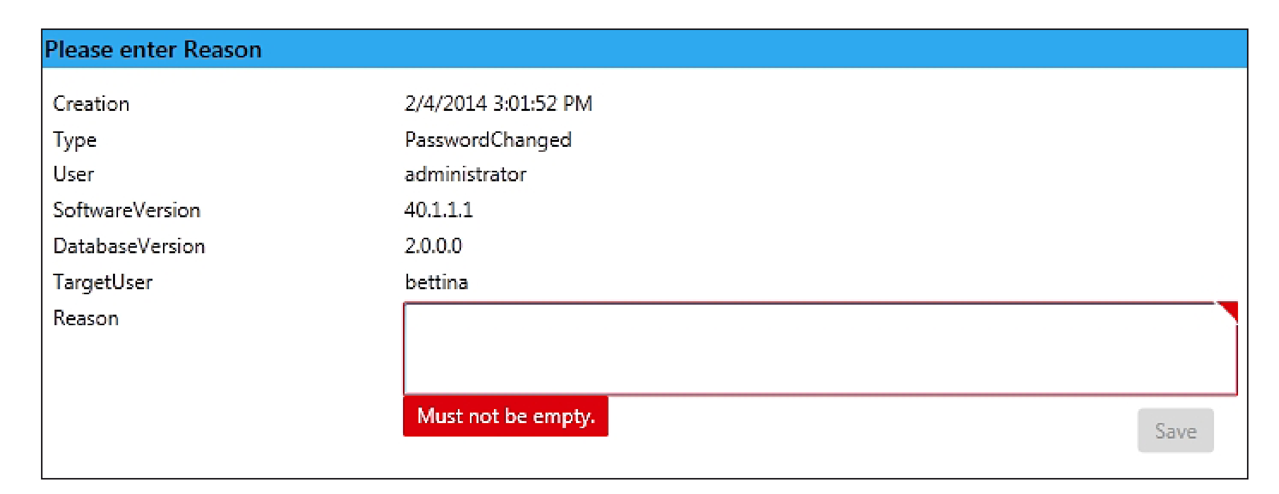


Abb. 5-1: Begründung eintragen

Wenn Sie Aktionen durchführen, die Systemkonfiguration oder den Datenbestand verändern, müssen Sie die Aktion begründen. epBlue GxP speichert die Begründung zusammen mit den Daten der Aktion im Audit Trail.

6 Installation

6.1 GxP-Aktivierungslizenz anfordern



Wenn Sie einen Aufrüstsatz epBlue GxP bestellt haben, müssen Sie die Software epBlue GxP mit der Aktivierungslizenz freischalten.
Wenn Sie eine epMotion mit epBlue GxP bestellt haben, wurde die Aktivierungslizenz bereits bei Eppendorf in die Software geladen.

Voraussetzung
- epMotion und MultiCon sind von einem autorisierten Techniker installiert worden.
- Ein USB-Speichermedium ist mit dem MultiCon verbunden.
- epBlue GxP wurde gestartet.
- Ein Anwender der Benutzergruppen *Administrator* oder *Administrator Lab* ist angemeldet.

1. Auf das Symbol *Setting* klicken.
2. Registerkarte *License Management* wählen.
3. Button *Show computer information* drücken.

   Das Fenster *Computer Identity Information* erscheint.

Abb. 6-1: Fenster *Computer Identity Information*

4. Button *Save to file* drücken.
5. Ordner auf dem USB-Speichermedium wählen.
6. Button *Save* drücken.

   Eine Textdatei mit der Computeridentifizierung wird gespeichert.
7. Internetseite www.eppendorf.com/software-licensing aufrufen.
8. Auf der Internetseite registrieren.
9. Den Inhalt der Textdatei vom USB-Speichermedium in das vorgesehene Feld auf der Internetseite kopieren.

   Sie erhalten die GxP-Aktivierungslizenz innerhalb von 48 Stunden per E-Mail.

6.2 Aktivierungslizenz importieren

Voraussetzung

- Das USB-Speichermedium mit der Aktivierungslizenz ist mit dem MultiCon verbunden.
- Ein Anwender der Benutzergruppen *Administrator* oder *Administrator Lab* ist angemeldet.
- Die Registerkarte *License Management* im Bereich *Settings* ist geöffnet.

1. Button *Open license file* drücken.
2. Das Fenster *Open Eppendorf License* erscheint.
3. Aktivierungslizenz auf dem USB-Speichermedium wählen.
4. Button *Open* drücken.
   Die Aktivierungslizenz wird in die Software eingefügt.
5. epBlue GxP neu starten.

6.3 System einrichten

6.3.1 Als Administrator anmelden

In epBlue GxP ist ein Benutzerkonto der Benutzergruppe *Administrator* installiert. Mit diesem Benutzerkonto richten Sie die Software ein.



Abb. 6-2: Fenster *Welcome to epBlue*

1. epBlue GxP starten.
   Das Fenster *Welcome to epBlue* erscheint.
2. In epBlue GxP anmelden:
   - Username: *Administrator*
   - Password:Admin123!

   Sie sind als Administrator angemeldet.

6.3.2 epBlue GxP konfigurieren

Um Prozesse und Strukturen des Labors entsprechend den Anforderungen für GxP abzubilden, besitzt epBlue GxP eine erweiterte Benutzerverwaltung.



Nur ein Anwender der Benutzergruppe *Administrator* hat die Berechtigung epBlue GxP zu konfigurieren.

Bevor Sie mit epBlue GxP arbeiten, nehmen Sie folgende Einstellungen vor:

- Passwort für das Benutzerkonto *Administrator* ändern.
  Neues Passwort sicher aufbewahren.
- Benutzerkonten einrichten.
- Sicherheit für Benutzerkonten einstellen.
- Signaturberechtigung für Benutzerkonten einstellen.
- Autorisierungsschema von Applikationen und Protokollen einstellen.

7 Bedienung

7.1 Anmelden und Passwort ändern

7.1.1 In epBlue GxP anmelden



Abb. 7-1: Fenster *Welcome to epBlue*

1. epBlue GxP starten.

   Das Fenster *Welcome to epBlue* erscheint.

2. Name und Passwort eintragen.
3. Button *Login* drücken.

   Sie sind in epBlue GxP angemeldet.

7.1.2 epBlue GxP entsperren

Wenn Sie eine definierte Zeit keine Eingaben machen, wird epBlue GxP gesperrt.



Abb. 7-2: epBlue GxP entsperren

- Passwort des angemeldeten Anwenders im Fenster *Unlock* eingeben.

  Wenn Sie beim Entsperren von epBlue GxP das Passwort mehrfach falsch eingeben, wird das Benutzerkonto nicht gesperrt.

7.1.3 Eigenes Passwort ändern

Wenn Ihr Passwort abgelaufen ist oder Sie Ihr Passwort ändern möchten, können Sie selbst ein neues Passwort vergeben.

Wenn Sie Ihr Passwort vergessen haben oder Ihr Benutzerkonto gesperrt ist, muss ein Anwender der Benutzergruppe *Administrator* ein neues Passwort vergeben.

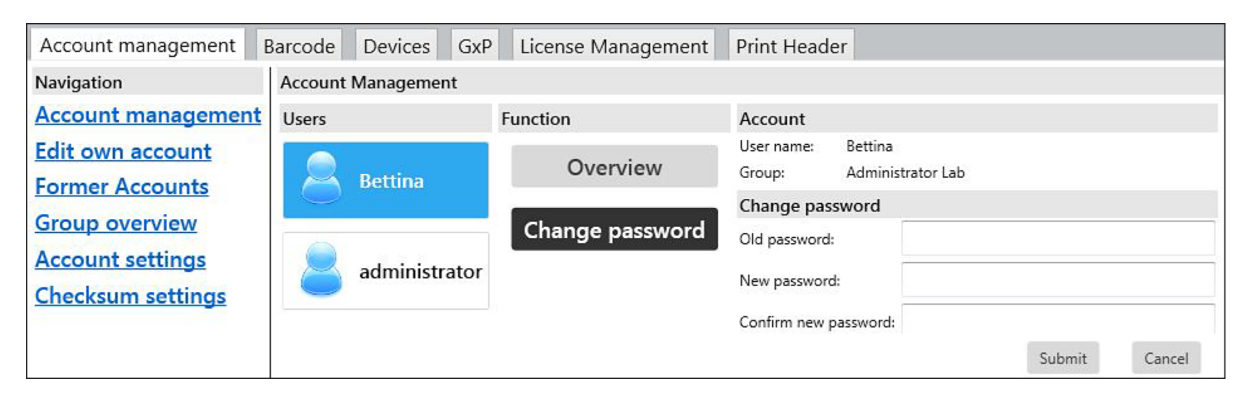


Abb. 7-3: Eigenes Passwort ändern

Voraussetzung
- Sie sind in epBlue GxP angemeldet.

1. Im Bereich *Settings* auf die Registerkarte *Account Management* > *Edit own account* klicken.
2. In der Spalte *Users* das Benutzerkonto markieren.
3. Button *Change Password* drücken.
4. Passwort im Feld *Old Password* eingeben.
5. Neues Passwort im Feld *New Password* eingeben.
6. Passwort im Feld *Confirm Password* noch einmal eingeben.
7. Um die Eingaben zu speichern, Button *Submit* drücken.

7.2 Digitale Signaturen verwenden

7.2.1 Applikationen signieren

Signaturen beziehen sich auf eine Revision.

Wenn sich eine Revision nicht im Status *authorized* befindet, können Sie die Revision nachträglich signieren.

Jede Signatur hat eine Bedeutung. Eine Bedeutung kann nur ein Mal pro Revision vergeben werden. Welche Bedeutungen zur Verfügung stehen hängt davon ab, welche Signaturen die Revision schon besitzt.

Welche Signaturen der Anwender vergeben kann, hängt von der Benutzergruppe des Anwenders ab.

Ein Anwender, der nicht in epBlue GxP angemeldet ist, kann eine Signatur ausführen.

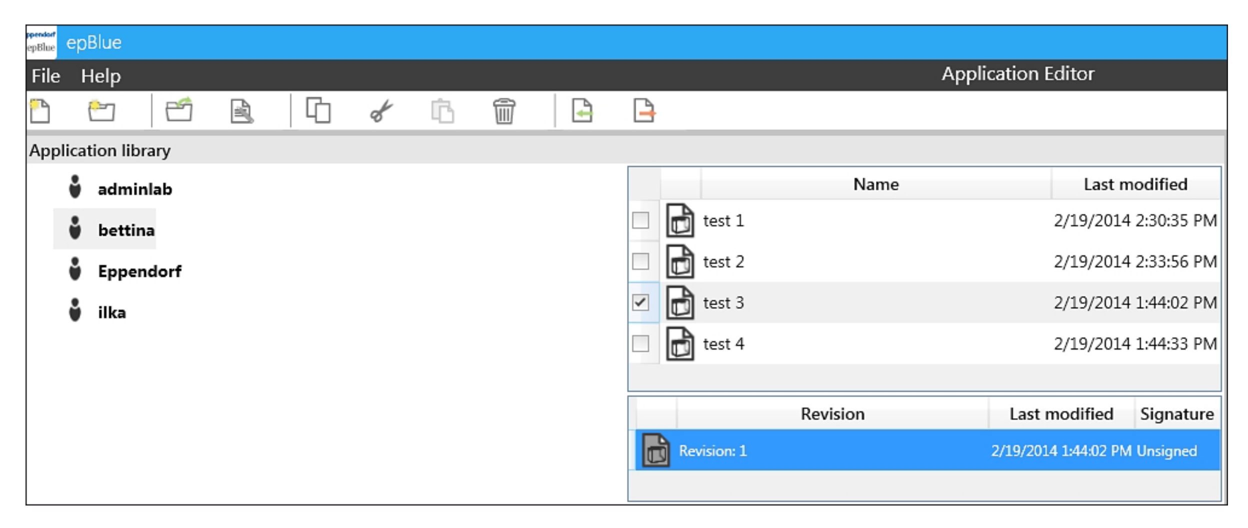


Abb. 7-4: Applikationen im *Application Editor*

Signieren Sie eine Revision folgendermaßen:

1. In epBlue GxP den Bereich *Application Editor* öffnen.
2. Applikation markieren.
3. Im Bereich *Revision* die Revision wählen.
4. In der Menüleiste auf das 🗁 klicken.

   Die Applikation wird geöffnet.
5. In der Menüleiste auf das Symbol 🖉 klicken.

   Das Fenster *Sign* öffnet sich.
   Wenn die Revision Signaturen besitzt, erscheinen die Signaturen im Fenster *Sign*.

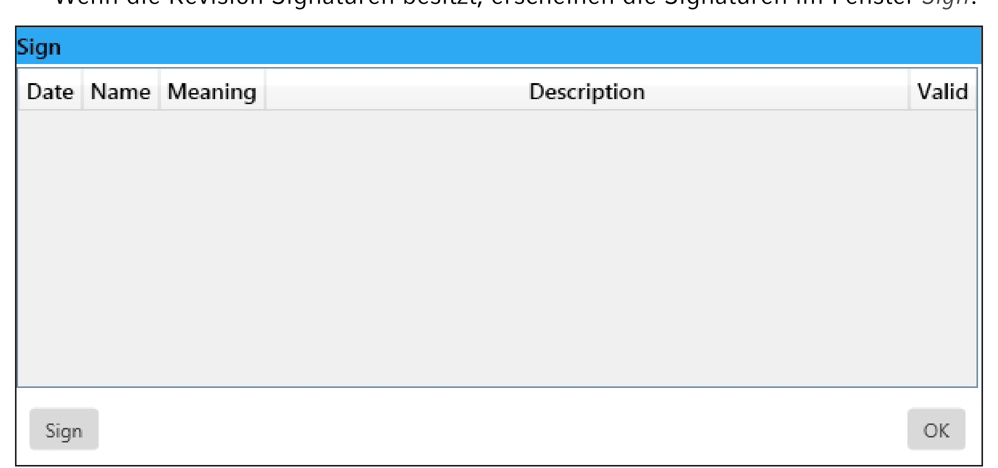


Abb. 7-5: Fenster *Sign*

6. Auf den Button *Sign* klicken.

   Das Fenster *Sign* öffnet sich.

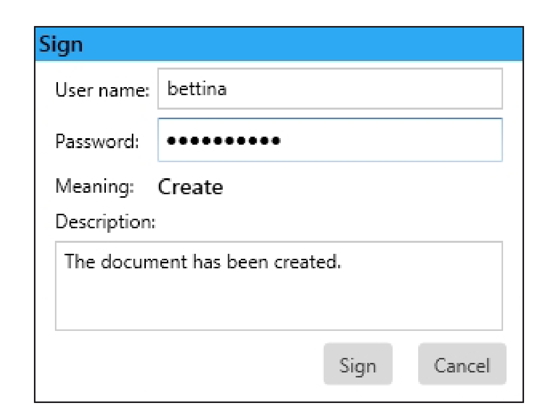


Abb. 7-6: Fenster *Sign*

User Identification
Name des signierenden Anwenders

Password
Passwort des signierenden Anwenders

Meaning
Bedeutung der Signatur

Description
Beschreibung der Signatur

7. Felder des Fensters *Sign* ausfüllen.
8. Um die Signatur zu speichern, auf den Button *Sign* klicken.

   Die Signatur erscheint im Fenster *Sign*.

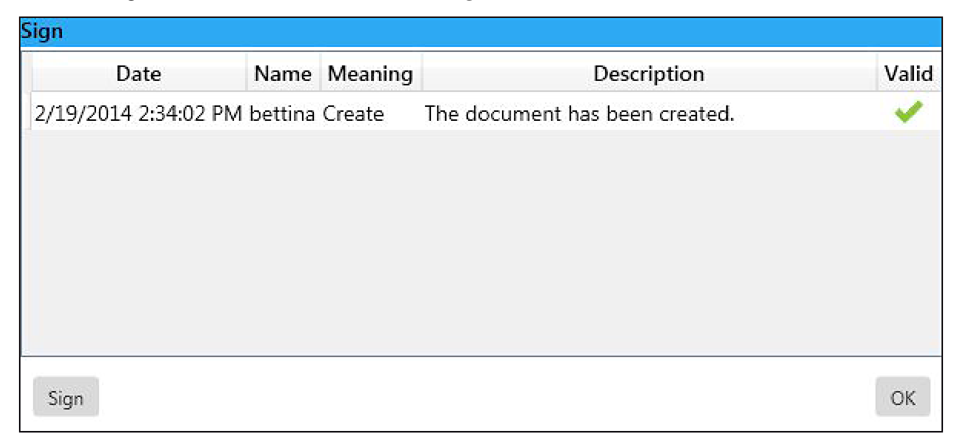


Abb. 7-7: Signatur einer Revision

9. Um weitere Signaturen einzufügen, auf den Button *Sign* klicken. Die beschriebenen Schritte wiederholen.
10. Fenster schließen. Dazu auf den Button *OK* klicken.

7.2.2 Protokolle signieren

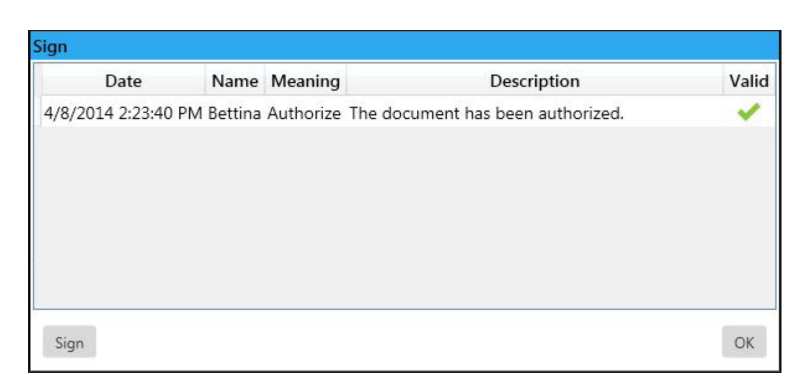


Abb. 7-8: Fenster *Sign*

Voraussetzung

- Die Revision besitzt den Status *authorized*.

1. Applikation mit Status *authorized* starten.

   Die Applikation wird ausgeführt. Wenn die Applikation beendet oder abgebrochen wurde, öffnet sich das Fenster *Sign Logfile*.

2. Auf den Button *Sign* klicken.

   Das Fenster *Sign* öffnet sich.

3. Felder ausfüllen, wie im Kapitel *Applikationen signieren* beschrieben, (siehe S. 30).
4. Auf den Button *Sign* klicken.

   Die Signatur erscheint im Fenster *Sign*.

5. Um das Fenster *Sign Logfile* zu schließen, auf den Button *OK* drücken.

7.2.3 Revisionen verwalten

epBlue GxP besitzt eine Revisionsverwaltung für Applikationen. Mit den Revisionen wird die Entwicklung der Applikation dokumentiert.

7.2.3.1 Aktuelle Revision öffnen

Sie können aktuelle Revisionen ändern.

1. In epBlue GxP den Bereich *Application Editor* öffnen.
2. Applikation markieren.
3. Auf das Symbol *Open application* klicken

   Die aktuelle Revision der Applikation wird geöffnet.

7.2.3.2 Beliebige Revision öffnen

Sie können jede Revisionen öffnen.

Ältere Revisionen können nicht verändert werden und werden im Status read-only geöffnet. Ältere Revisionen sind solange ausführbar, bis die aktuelle Revision den Status *authorized* besitzt.

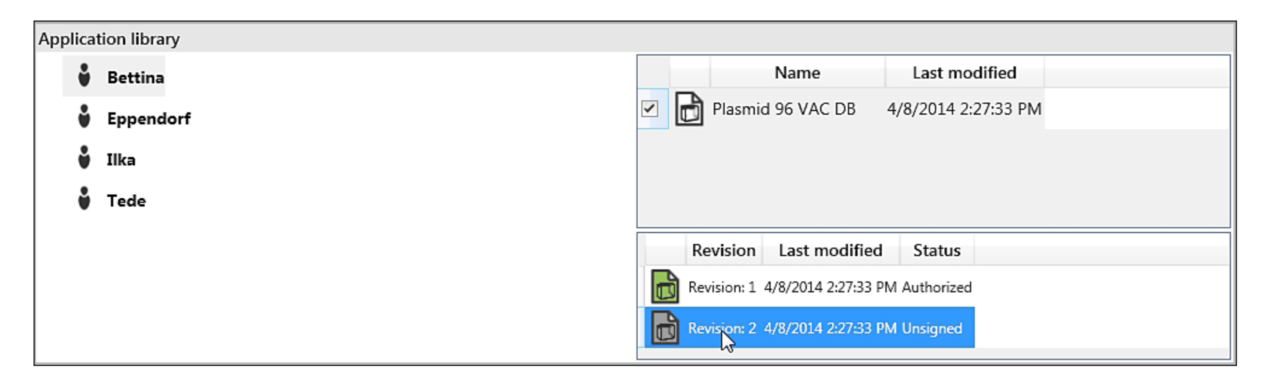


Abb. 7-9: Revision öffnen

1. In epBlue GxP den Bereich *Application Editor* öffnen.
2. Applikation markieren.
3. Im Bereich *Revision* die Revision wählen.
4. In der Menüleiste auf das Symbol 🗁 klicken.
   Die Revision wird geöffnet.
   Revision werden in der Spalte *Open Applications* angezeigt.



Abb. 7-10: Informationen über die geöffnete Revision

7.2.3.3 Neue Revision anlegen

Signierte Applikationen sind schreibgeschützt und können nicht geändert werden. Um eine signierte Applikation zu ändern, müssen sie eine neue Revision anlegen.

Legen Sie eine neue Revision folgendermaßen an:

Voraussetzung
- Die aktuelle Revision besitzt mindestens eine Signatur.

1. In epBlue GxP den Bereich *Application Editor* öffnen.
2. Applikation markieren.
3. Im Bereich *Revision* die Revision wählen.
4. Auf das Symbol *Open application* klicken.
   Die Revision wird geöffnet.

5. In der Menüleiste auf das Symbol klicken.
   Eine neue nicht signierte Revision wird angelegt.
6. Applikation ändern.
   Wenn Sie eine signierte Revision geändert haben, können Labware-Konflikte auftreten (siehe *Signierte Applikationen ändern auf S. 38)*.
7. Um die Revision zu speichern, auf den Button *Save* klicken.
8. Begründung für die Änderungen der Applikation eingeben.
9. Button *OK* drücken.
   Sie haben eine neue, nicht signierte Revision angelegt.

7.2.4 Signaturen
7.2.4.1 Signaturen von Applikationen anzeigen

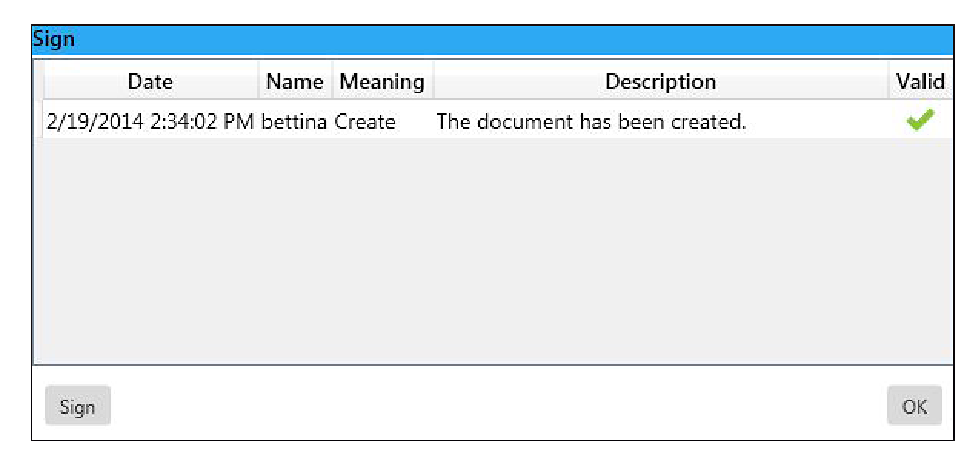


Abb. 7-11: Fenster *Sign*

1. In epBlue GxP den Bereich *Application Editor* öffnen.
2. Applikation markieren.
3. Im Bereich *Revision* die Revision wählen.
4. Auf das Symbol *Open application* klicken.
   Die Revision wird geöffnet.
5. In der Menüleiste auf das Symbol *Sign* klicken.
   Das Fenster *Sign* öffnet sich.

7.2.4.2 Signaturen von Protokollen anzeigen

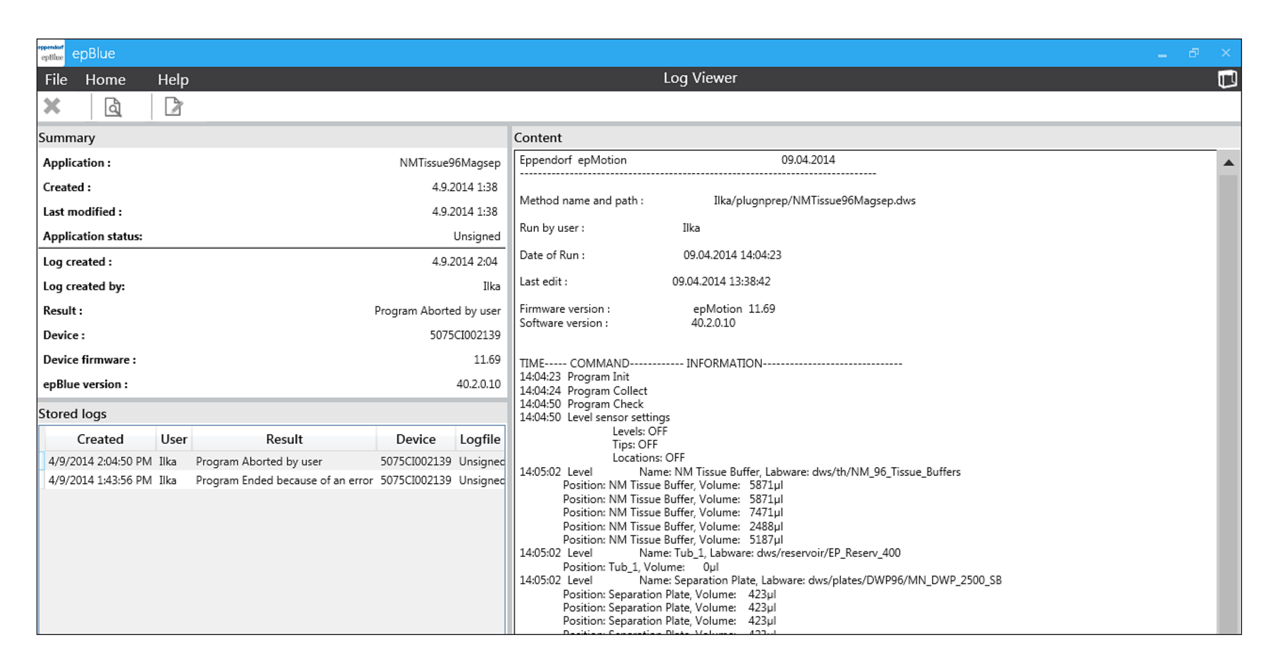


Abb. 7-12: Gespeicherte Protokolle im Fenster *LogViewer*

1. In epBlue GxP den Bereich *Log Viewer* öffnen.
2. Applikation markieren.
3. Im Bereich *Revision* die Revision wählen.
4. In der Menüleiste auf das Symbol 🗁 klicken.
   Die Protokolle, die zur gewählten Applikation gehören, werden geöffnet.
5. Im Bereich *Stored logs* Protokoll wählen.
6. Auf das Symbol *Show signatures* klicken.
7. Das Fenster *Sign* öffnet sich.

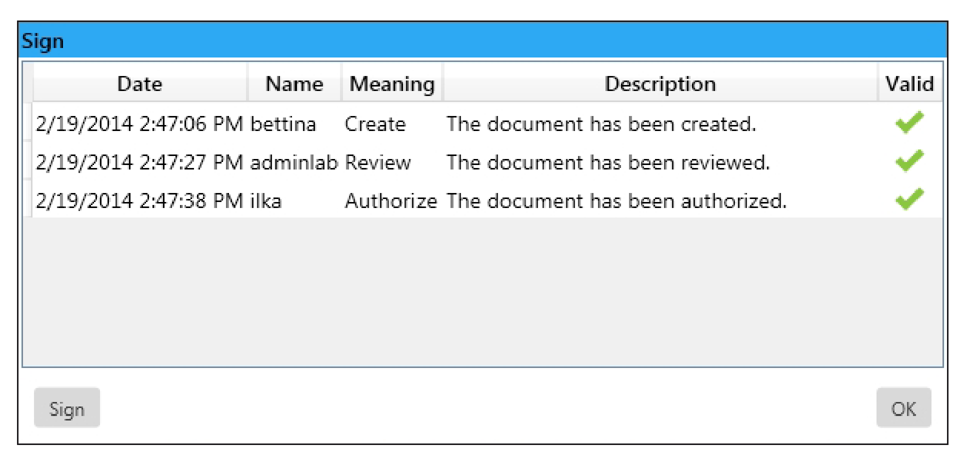


Abb. 7-13: Signaturen eines Protokolls

7.2.4.3 Signaturen prüfen

Wenn eine Signatur gültig ist, wurde das Dokument nach dem Signieren nicht verändert. Wenn die Signatur einer Applikation gültig ist, wurde die verwendete Labware nicht verändert.

Eine ungültige Signatur deutet auf eine Manipulation hin.

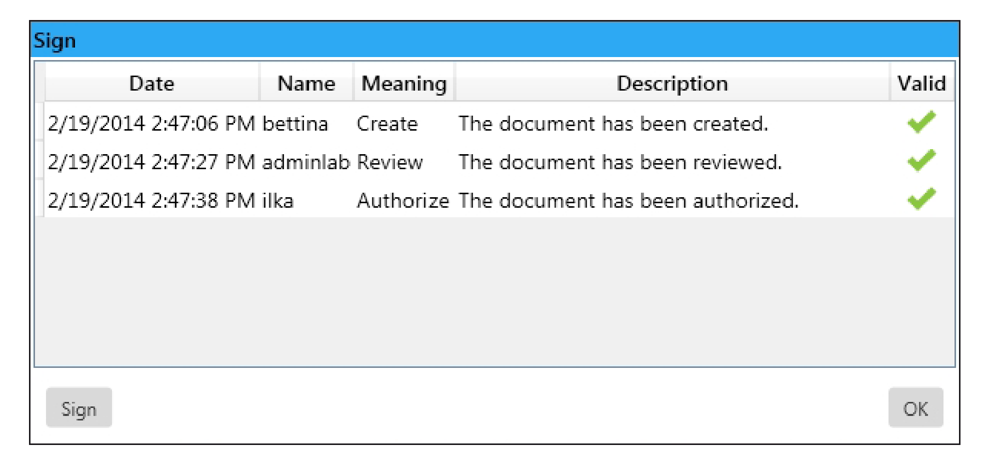


Abb. 7-14: Fenster *Sign*

Date
Datum und Uhrzeit des Signierens.

Name
Name des Anwenders, der das Dokument signiert hat.

Meaning
Bedeutung der Signatur.

Description
Status der Signatur.

Valid
Gültigkeit der Signatur:
✓ Signatur ist GÜLTIG.
✗ Signatur ist UNGÜLTIG.

Voraussetzung

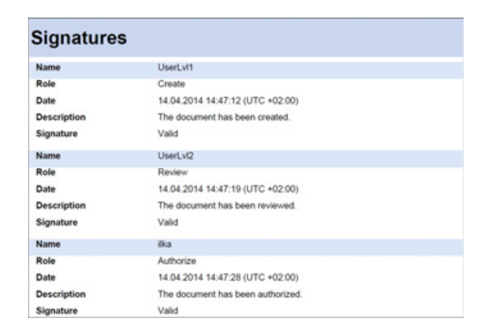
- Das Fenster *Sign* ist geöffnet.

▸ Signaturen prüfen.

Jede Zeile entspricht einer Signatur. Wenn das Dokument keine Signaturen besitzt, ist das Fenster leer.

7.2.5 Signaturen in Applikationen und Protokollen

Ausdrucke von Applikationen und Protokollen enthalten Status und Gültigkeit der Signatur.



Signatures

Name	UserLvl1
Role	Create
Date	14.04.2014 14:47:12 (UTC +02:00)
Description	The document has been created.
Signature	Valid
Name	UserLvl2
Role	Review
Date	14.04.2014 14:47:19 (UTC +02:00)
Description	The document has been reviewed.
Signature	Valid
Name	ilka
Role	Authorize
Date	14.04.2014 14:47:28 (UTC +02:00)
Description	The document has been authorized.
Signature	Valid

Abb. 7-15: Informationen zur Signatur im Ausdruck

7.3 Labware in signierten Applikationen

epBlue GxP speichert eine Momentaufnahme der verwendeten Labware zusammen mit der signierten Applikation. Signierte Applikationen können ausgeführt werden, auch wenn die Labware in der Labware-Bibliothek geändert wird. Die signierte Applikation wird mit der Momentaufnahme der Labware ausgeführt, die in der Applikation gespeichert ist.

7.3.1 Signierte Applikationen ändern

Wenn Sie eine neue Revision von einer signierten Applikation anlegen, übernimmt epBlue GxP die Momentaufnahme der Labware in die Revision und vergleicht sie mit der Labware in der Labware-Bibliothek. Wenn die Labware, von der die Momentaufnahme erzeugt wurde, in der Labware-Bibliothek verändert oder gelöscht wurde, entsteht ein Labware-Konflikt. epBlue GxP bietet verschiedene Lösungen für Labware-Konflikte.

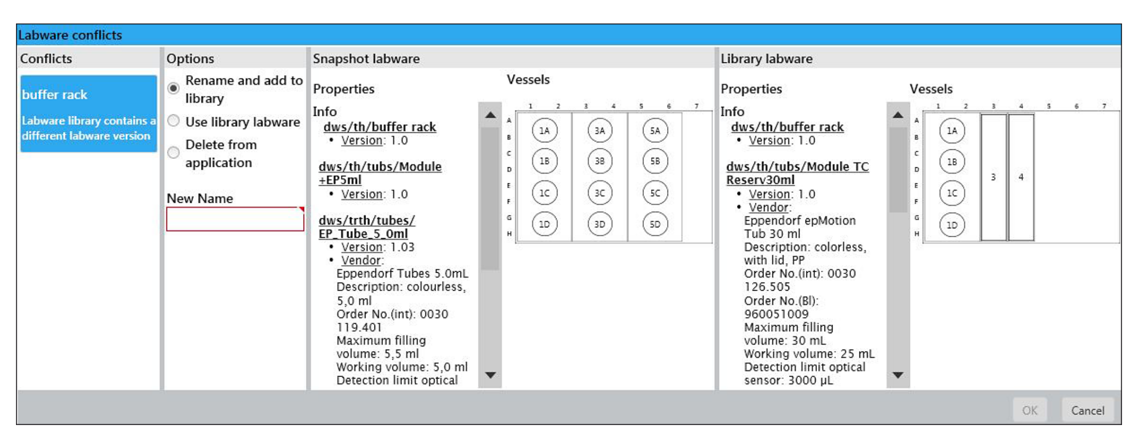


Abb. 7-16: Fenster *labware conflicts*

Spalte *Conflicts*
Labware-Konflikt.

Spalte *Options*
Möglichkeiten, den Labware-Konflikt zu lösen.

Spalte *Snapshot Labware*
Eigenschaften der Labware, die in der signierten Applikation verwendet wird.

Spalte *Library Labware*
Eigenschaften der Momentaufnahme der Labware.

Neue Revision anlegen

1. Neue Revision der Applikation anlegen.
2. Alternativ die Applikation unter einem anderem Namen speichern.

   Wenn ein Labware-Konflikt entsteht, erscheint das Fenster *labware conflicts*. In diesem Fenster zeigt epBlue GxP Probleme und Lösungen für den Labware-Konflikt.

Labware-Konflikt lösen

3. Möglichkeit wählen, mit der der Labware-Konflikt gelöst werden soll.

Möglichkeit, den Labware-Konflikt zu lösen	**Beschreibung**
Rename and add to library	• Unter dem Namen ist Labware mit dem gleichen Namen aber unterschiedlichen Eigenschaften vorhanden. • Die Momentaufnahme der Labware wird als neue Labware zur Labware-Bibliothek hinzugefügt. • Für die neue Labware muss ein Name vergeben werden. • Die Momentaufnahme der Labware wird in der neuen Revision verwendet. • Alle in der Applikation verwendeten Pattern bleiben gültig. • Die Applikation bleibt ohne Änderungen ausführbar.
Add labware to library	• Unter dem Namen ist keine Labware vorhanden. • Die Momentaufnahme der Labware wird zur Labware-Bibliothek hinzugefügt. • Die Momentaufnahme der Labware wird in der neuen Revision verwendet. • Alle in der Applikation verwendeten Pattern bleiben gültig, • Die Applikation bleibt ohne Änderungen ausführbar.
Use library labware	• Die Momentaufnahme der Labware wird durch Labware aus der Labware-Bibliothek ersetzt. • Wenn sich die Momentaufnahme der Labware und die Labware in der Labware-Bibliothek unterscheiden, werden Pattern ungültig. • Wenn sich die Momentaufnahme der Labware und die Labware in der Labware-Bibliothek unterscheiden, ist die Applikation ohne Änderungen nicht mehr ausführbar.
Delete from application	• Die Momentaufnahme der Labware wird gelöscht. • Pattern werden ungültig. • Die Applikation ist ohne Änderungen nicht mehr ausführbar.

7.4 Mit signierten PDF-Dokumenten arbeiten

Digital signierte PDF-Dokumente enthalten die Systemsignatur und die Signatur des Anwenders, der die PDF-Dokumente exportiert, sowie die zugehörigen Zertifikate. Die digitale Signatur ist als verschlüsselter Code untrennbar in das PDF-Dokument eingebettet.

epBlue GxP exportiert digital signierte PDF-Dokumente von folgenden Daten:

- Signierte Applikationen
- Signierte Protokolle
- Audit Trail
- IQ
- Archive bestehend aus Applikationen, Protokollen und darin verwendeter Labware

Daten in der Datenbank verändern sich durch das Exportieren nicht.

7.4.1 Daten als signierte PDF-Dokumente exportieren

Voraussetzung

- Sie sind in epBlue GxP als *Administrator* oder *Administrator Lab* angemeldet.
- In der Datenbank befinden sich Applikationen und Protokolle mit einer Signatur.

1. Bereich wählen, in dem sich die Daten befinden, die exportiert werden sollen.

Applikationen	**Protokolle**	**Audit Trail**	**IQ**
Bereich *Application Editor*	Bereich *Log Viewer*	Bereich *Audit Trail Viewer*	Bereich *Settings* > *Devices*

2. Daten markieren.
3. In der Menüleiste auf das Symbol klicken.
   Die Druckvorschau öffnet sich.
4. Auf den Button PDF klicken.
   Das Fenster *Sign* erscheint.

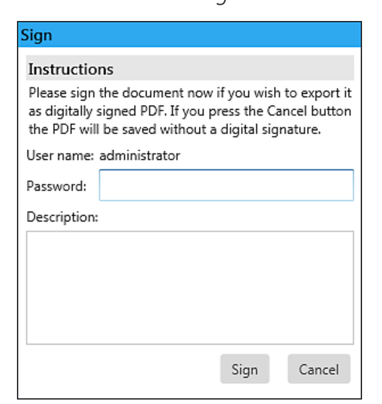


Abb. 7-17: Fenster *Sign*

Password
Passwort des Anwenders.

Description
Begründung für den Export der Daten eingeben.

5. Wenn das PDF-Dokument nicht signiert werden soll, auf den Button *Cancel* klicken.
6. Um das PDF-Dokument zu signieren, auf den Button *Sign* klicken.
7. Wählen, wohin das PDF-Dokument gespeichert werden soll.
8. Auf den Button *Save* klicken.

7.4.2 Digitale Zertifikate aus epBlue GxP exportieren

Um die Signaturen in PDF-Dokumenten zu prüfen, benötigen Sie exportierte digitale Zertifikate.



Das Master-Zertifikat befindet sich auf der Internetseite www.eppendorf.com/automation.



Abb. 7-18: Fenster *Certificates*

Voraussetzung

- Sie sind in epBlue GxP als *Administrator* angemeldet.

1. Bereich *Settings* öffnen.
2. In der Registerkarte *GxP* auf den Eintrag *Certificates* klicken.
3. Im Bereich *Certificates* die Zertifikate wählen, die exportiert werden sollen.

Master	Das Master-Zertifikat wird exportiert.
System	Das Systemzertifikat wird exportiert.
All	Die Zertifikate aller Anwender, das Master-Zertifikat und das Systemzertifikat werden exportiert. Die Zertifikate deaktivierter und gelöschter Benutzerkonten werden exportiert.

4. Auf den Button *Export* klicken.
   Das Fenster *Browse For Folder* öffnet sich.
5. Wählen, wohin die Zertifikate gespeichert werden sollen. Auf den Button *OK* klicken.

Jedes Zertifikat wird im Format PKCS#7 (*.cer) gespeichert.



Wenn ein Anwender der Benutzergruppe *Administrator* das Passwort eines Benutzerkontos geändert hat, werden für dieses Benutzerkonto mehrere digitale Zertifikate exportiert. Um die Signaturen des Anwenders vor und nach der Änderung des Passworts zu prüfen, benötigen Sie alle digitalen Zertifikate.

- Archivieren Sie alle digitalen Zertifikate eines Anwenders.

7.4.3 Master-Zertifikat in PDF-Anzeigeprogramm importieren

Um die Gültigkeit der Signaturen und Zertifikate in einem PDF-Anzeigeprogramm zu prüfen, müssen Sie das Master-Zertifikat aus epBlue GxP exportieren und in das PDF-Anzeigeprogramm importieren.

Das Masterzertifikat ist das Stammzertifikat von epBlue GxP. Das Systemzertifikat und die Zertifikate der Anwender sind mit dem Master-Zertifikat signiert.



Der Umgang mit Zertifikaten ist in jedem PDF-Anzeigeprogramm anders. Details finden Sie in der Anleitung Ihres PDF-Anzeigeprogramms.
Viele PDF-Anzeigeprogramme vertrauen Zertifikaten, die von einem vertrauenswürdigen Stammzertifikat stammen, z.B. Adobe Reader.

Wenn Ihr PDF-Anzeigeprogramme dem Master-Zertifikat vertraut, gehen Sie folgendermaßen vor, um das Master-Zertifikat zu importieren.

Voraussetzung

- Das Master-Zertifikat befindet sich in der Datei *MasterCertificate.cer* (siehe *Zertifikate auf S. 23)*.
- Das PDF-Anzeigeprogramm unterstützt Zertifikate im Format PKCS #7.

1. Datei *MasterCertificate.cer* in das PDF-Anzeigeprogramm importieren.
   Das Master-Zertifikat wurde unter der Bezeichnung *Eppendorf epBlue CA* importiert.
2. Master-Zertifikat prüfen.
   Die Prüfsummen müssen folgender Zeichenfolge entsprechen. Die Zeichenfolge kann Großbuchstaben oder Kleinbuchstaben enthalten.

Tab. 7-1: Prüfsumme für Zeichenfolgen

SHA1-Digest	9E B7 33 3D 2A 8D 16 D3 82 C4 01 B8 AD A2 8B FF BF B8 87 70
MD5-Digest	47 90 88 69 77 44 B2 DB A2 AE 41 29 FF 1C EF 59

3. Um Signaturen in PDF-Dokumenten aus epBlue GxP zu prüfen, legen Sie folgende Einstellung fest.
   - Das Master-Zertifikat als vertrauenswürdiges Stammzertifikat verwenden.
   - Dem Master-Zertifikat für die Signatur von Dokumenten vertrauen.
   - Dem Master-Zertifikat für die Zertifizierung von Dokumenten vertrauen.

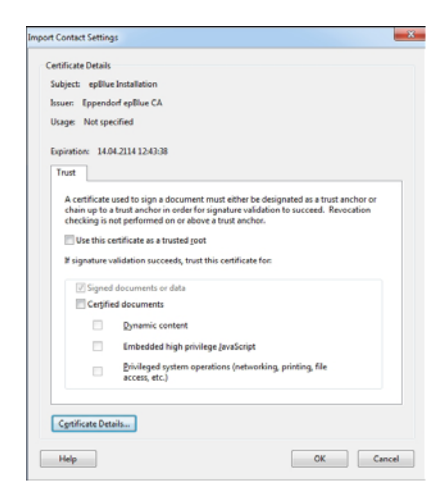


Abb. 7-19: Einstellungen des Master-Zertifikats in Adobe Reader

7.4.4 Signaturen und Zertifikate in PDF-Dokumenten prüfen

Um Signaturen zu prüfen Sie können jedes PDF-Anzeigeprogramm verwenden, das PKCS #7 Zertifikate unterstützt. Im Folgenden ist die Arbeitsweise mit dem Adobe Reader 9 dargestellt.

Voraussetzung

- Das Master-Zertifikat wurde in das PDF-Anzeigeprogramm importiert (siehe *Master-Zertifikat in PDF-Anzeigeprogramm importieren auf S. 42)*.

1. PDF-Dokument öffnen.
2. Auf den Button *Signature Panel* klicken.

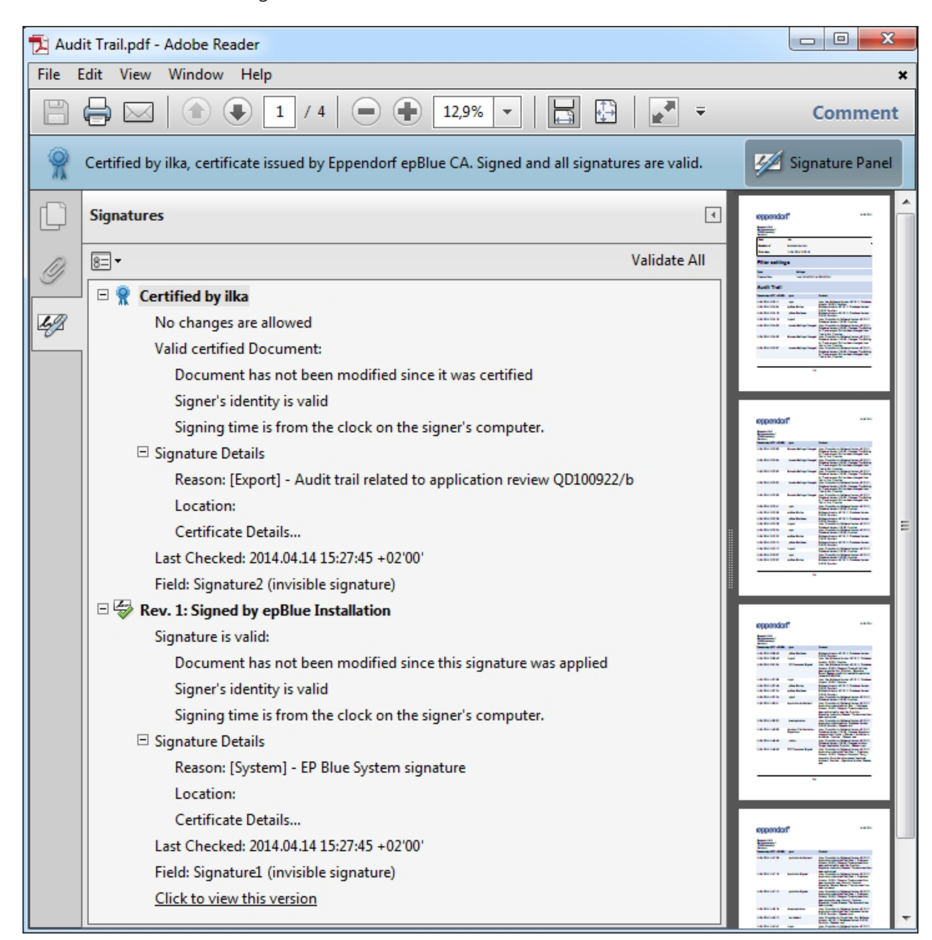


Abb. 7-20: Zertifikat im Adobe Reader

3. Gültigkeit der Signaturen prüfen.
4. Um eingebundene Zertifikate anzusehen, auf den Button *Certificate Details...* klicken.

   Wenn das Dokument vom signierenden Anwender aus epBlue GxP exportiert wurde (Authentizität) und das Dokument nicht verändert wurde (Integrität) sind die Signaturen gültig.

7.5 Audit Trail

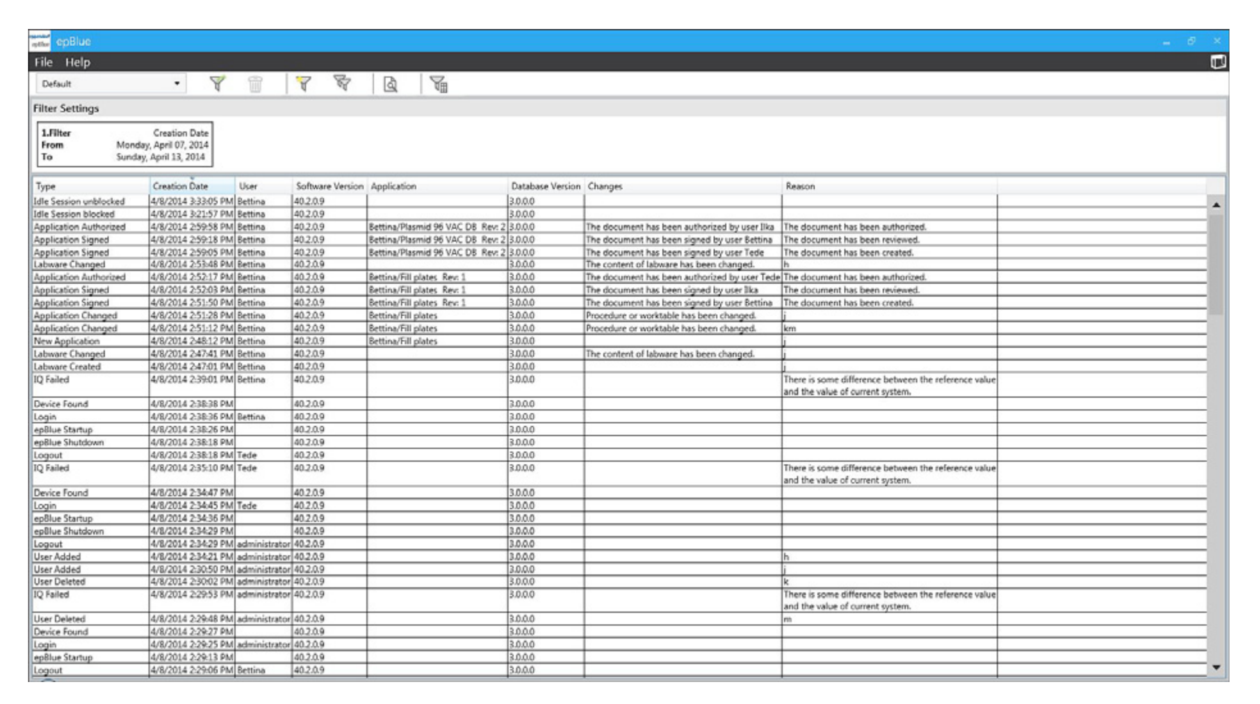


Abb. 7-21: Audit Trail



Der Zeitstempel zeigt die Uhrzeit entsprechend der Zeitzone in der Systemkonfiguration des Betriebsystems. Wenn die Zeitzone geändert wird, werden die Zeitstempel automatisch angepasst. Die eingestellte Zeitszone ist im Ausdruck des Audit Trail enthalten.

7.5.1 Audit Trail öffnen

- In epBlue GxP den Bereich *AuditTrail Viewer* öffnen.
  Der Audit Trail wird als Tabelle dargestellt. Jede Zeile zeigt einen Eintrag.

7.5.2 Details eines Eintrags zeigen

- Eintrag in der Tabelle markieren.
  Die Details erscheinen im Bereich *Selected entry*.

7.5.3 Einträge sortieren

1. Kopf der Spalte anklicken, nach der sortiert werden soll.
   Die Tabelle wird aufsteigend sortiert.
2. Um absteigend zu sortieren, Kopf der Spalte erneut anklicken.

7.5.4 Filter erstellen

1. Auf das Symbol *New Filter* klicken.
   Das Fenster *Filter* erscheint.
2. Namen für den Filter festlegen.
3. Filterkriterien definieren.
4. Mit dem Button *Add* weitere Filterkriterien hinzufügen.
5. Um den Filter zu speichern, Button *Save* drücken.

7.5.5 Filter bearbeiten

1. Auf das Symbol *Edit Filter* klicken.
   Das Fenster *Filter* erscheint.
2. Ggf. Namen des Filters ändern.
3. Filterkriterien ändern.
   Mit dem Button *Add* Filterkriterien hinzufügen.
   Mit dem Button *Remove* Filterkritirien löschen
4. Um den Filter zu speichern, Button *Save* drücken.

7.5.6 Filter wählen

- Im Dropdownmenü der Menüleiste Filter wählen.
  Der Audit Trail wird dem Filter angepasst.

7.5.7 Filter löschen

1. Im Dropdownmenü der Menüleiste den Filter wählen.
   Der Audit Trail wird dem Filter angepasst.
2. Um den geöffneten Filter zu löschen, auf das Symbol *Papierkorb* drücken.

7.5.8 Sichtbare Spalten wählen

- Dropdownmenü *Select Visible Columns* öffnen.
- Spalten markieren, die gezeigt werden sollen.

7.5.9 Audit Trail drucken und exportieren

Sie können den angezeigten Teil des Audit Trail drucken oder als PDF-Dokument exportieren.

1. Audit Trail aufrufen.
2. Ggf. Filter wählen.
3. Symbol drücken.
   Die Druckvorschau öffnet sich.
4. Um den Audit Trail auszudrucken, in der Druckvorschau auf das Symbol klicken.
5. Um den Audit Trail als PDF-Dokument zu exportieren, in der Druckvorschau auf den Button PDF drücken.

7.5.10 Kategorien des Audit Trail

Ereignisse werden als Einträge im Audit Trail gespeichert. Jedes Ereignis, das einen Eintrag erhält, wird einer Kategorie zugeordnet.

Tab. 7-2: Anwenderdaten ändern

Kategorie	Ereignis
New Application *Application Changed* *Application Deleted* *Application Saved Under New Name* *Application Imported* *Application Exported* *Application Printed*	• Der Anwender hat eine neue Applikation erstellt. • Der Anwender hat eine bestehende nicht signierte Applikation geändert, gelöscht oder unter einem neuen Namen gespeichert. • Der Anwender hat eine Applikation importiert oder exportiert. • Der Anwender hat eine Applikation gedruckt oder als PDF-Dokument exportiert.
Old Application Updated	• Der Anwender hat im *Application Editor* bestätigt, dass er eine importierte Applikation aktualisieren will, die mit einer älteren Version der Software erzeugt wurde.
Official Application Changed *Official Application Copied*	• Der Anwender hat eine signierte Applikation geändert und damit eine neue nicht signierte Revision erzeugt. • Der Anwender hat eine signierte Applikation kopiert.
Application Signed *Application Authorized*	• Der Anwender hat eine Applikation als *created* oder *reviewed* signiert. • Der Anwender hat eine Applikation als *authorized* signiert.
Application Log Printed	• Der Anwender hat ein Protokoll gedruckt oder als PDF-Dokument exportiert.
Labware Created *Labware Changed* *Labware Deleted* *Labware Copied* *Labware Imported* *Labware Exported* *Labware Printed*	• Der Anwender hat neue Labware erstellt. • Der Anwender hat bestehende Labware geändert, gelöscht oder kopiert. • Der Anwender hat Labware importiert oder exportiert. • Der Anwender hat Labware gedruckt oder als PDF-Dokument exportiert.
ID list created *ID list exported* *ID list removed*	epBlue ID • Der Anwender hat eine ID-Liste erzeugt. Die ID-Liste wurde beim Importieren einer Datei oder bei der Ausführung einer Applikation mit ID-Verfolgung erzeugt. • Der Anwender hat eine ID-Liste exportiert. • Der Anwender hat eine ID-Liste entfernt.
Archive	• Ein Anwender der Benutzergruppe *Administrator* hat eine oder mehrere Applikationen oder Teile des Audit Trail archiviert.

Tab. 7-3: Applikationen ausführen

Kategorie	Ereignis
Application Started *Application Ended*	• Der Anwender hat eine Applikation gestartet. • Eine Applikation wurde beendet.
Number of Samples	• Der Anwender hat die Zahl der Proben für eine Applikation manuell eingegeben.
Application Stopped *Singlestep Application* *Continue Application*	• Der Anwender hat eine Applikation angehalten. • Der Anwender hat einen Schritt im angehaltenen Lauf ausgeführt. • Eine Applikation wurde fortgesetzt.
Application Error	• Während einer Applikation ist ein Fehler aufgetreten.
Application Aborted	• Eine Applikation wurde abgebrochen.

Tab. 7-4: Benutzerkonten und Aktionen des Anwenders

Kategorie	Ereignis
Login *Logout*	• Ein Anwender hat sich bei epBlue GxP angemeldet oder abgemeldet.
Idle Session blocked *Idle Session unblocked*	• epBlue GxP wurde gesperrt. Der Anwender hat eine definierte Zeit keine Eingaben gemacht hat. • Ein Anwender hat epBlue GxP durch Eingabe seines Passworts entsperrt.
Used added *User deleted* *User Group Changed* *Password Changed*	• Ein Anwender der Benutzergruppe *Administrator* hat ein Benutzerkonto neu angelegt oder gelöscht. • Ein Anwender der Benutzergruppe *Administrator* hat ein Benutzerkonto einer anderen Benutzergruppe zugewiesen. • Ein Anwender hat sein Passwort geändert oder ein Anwender der Benutzergruppe *Administrator* hat ein neues Passwort für einen Anwender festgelegt.
False Login User Disabled	• Der Anwender hat mehrfach ein falsches Passwort eingegeben. Das Benutzerkonto wurde gesperrt.
Disabled User Reactivated	• Ein Anwender der Benutzergruppe *Administrator* hat ein gesperrtes Benutzerkonto entsperrt.
Password Expired	• Die Gültigkeit eines Passworts ist abgelaufen.
Account Expired	• Die Gültigkeit eines Benutzerkontos ist abgelaufen.

Tab. 7-5: System einstellen und ändern

Kategorie	Ereignis
Device Found *Device Added* *Device Lost*	• epBlue GxP hat ein angeschlossenes Gerät erkannt. • epBlue GxP hat eine epMotion 5075 erkannt und zur Auswahl hinzugefügt. • Die Kommunikation zwischen epBlue GxP und einer epMotion 5075 wurde unterbrochen.
Device Initialization Failed	• epBlue GxP konnte ein angeschlossenes Gerät nicht initialisieren.
Device Status Changed	• Der Status des Geräts hat sich geändert, z.B. durch Starten oder Beenden einer Applikation.
Device Firmware Update	• Ein Anwender der Benutzergruppen *Administrator Lab* oder *Service* hat eine andere Firmware-Version der epMotion 5075 installiert.
Barcode Settings Changed	epBlue ID • Ein Anwender der Benutzergruppe *Administrator Lab* hat Einstellungen des Barcode-Readers geändert.
Number of reagent IDs changed *Import/Export Settings for ID List Changed*	epBlue ID • Ein Anwender der Benutzergruppe *Administrator Lab* hat die Anzahl der erforderlichen IDs oder Barcodes für Reagenzien geändert. • Ein Anwender der Benutzergruppe *Administrator Lab* hat das Dateiformat oder Speicherort für den Import oder Export von ID-Listen geändert.
Checksum Settings changed	epBlue ID • Ein Anwender der Benutzergruppe *Administrator* oder *Administrator Lab* hat die Einstellung zur Kontrolle der Prüfsumme von ID-Listen oder CSV-Dateien geändert.
Number of Authorization Signatures	• Ein Anwender der Benutzergruppe *Administrator* hat das Autorisierungsschema von Applikationen oder Protokollen geändert.
Password Lifetime Changed *Maximum Login Retries Changed* *Max Idle Time Changed*	• Ein Anwender der Benutzergruppe *Administrator* hat die Dauer der Gültigkeit für Passwörter von Benutzerkonten geändert. • Ein Anwender der Benutzergruppe *Administrator* hat die Zahl fehlgeschlagener Anmeldungen geändert, nach der ein Benutzerkonto gesperrt wird. • Ein Anwender der Benutzergruppe *Administrator* hat die Zeit geändert, nach der ein Benutzerkonto gesperrt wird, wenn der Anwender keine Aktionen durchgeführt hat.
Auto-Backup *Database successfully restored*	• epBlue GxP hat eine automatische Sicherung durchgeführt. Bei der Durchführung der automatischen Sicherung ist ein Fehler aufgetreten. • Ein Anwender der Benutzergruppe *Administrator* hat die epBlue-Datenbank aus einer Sicherung wiederhergestellt.
Dialog Message	• epBlue GxP hat eine Meldung angezeigt.
epBlue Application Error	• Bei der Erstellung einer digitalen Signatur ist ein Fehler aufgetreten. • Ein Softwarefehler ist aufgetreten.
Device Configuration Changed *Service Function*	• Der autorisierte Service hat die Konfiguration des Geräts geändert. • Der autorisierte Service hat eine Funktion zur Prüfung ausgeführt oder eine Einstellung des Geräts verändert.

7.6 Prüfsummen erstellen und prüfen

Mit Prüfsummen werden Dateien kontrolliert, die zwischen epBlue GxP und anderen Programmen ausgetauscht werden. Damit werden Fehler bei der Datenübertragung und Manipulationen an Daten erkannt. Sie können die Prüfsumme von Dateien beim Importieren in epBlue GxP oder in externer Software kontrollieren.

7.6.1 Dateien mit Prüfsummen importieren und prüfen



epBlue GxP kann die Prüfsummen von Dateien nicht kontrollieren, wenn die Dateien das Format zip, dws, lhs und ws besitzen und aus älteren Versionen von epBlue GxP oder aus dem epMotion 5075 Control Panel stammen.

Wenn Sie folgende Daten importieren, prüft epBlue GxP die Prüfsummen.

<table>
<tr><th>Dateiformat</th><th>Anwendung</th><th>Prüfsumme</th></tr>
<tr><td>.export</td><td>• Applikationen
• Labware</td><td>• Die Prüfsumme wird immer kontrolliert.</td></tr>
<tr><td>.csv</td><td>• Applikationen
• ID-Listen</td><td rowspan="2">• Wenn die Kontrolle der Prüfsumme aktiviert wurde, kontrolliert epBlue GxP die Prüfsumme.
• Wenn die Kontrolle der Prüfsumme nicht aktiviert wurde, ignoriert epBlue GxP eine vorhandene Prüfsumme.</td></tr>
<tr><td>.xml</td><td>• ID-Listen</td></tr>
</table>

Voraussetzung

- Die Kontrolle der Prüfsumme ist aktiviert.

▸ Dateien importieren, wie in der Software-Bedienungsanleitung beschrieben.
  Wenn die Kontrolle der Prüfsumme erfolgreich war, wird die Datei importiert.
  Wenn die Prüfsumme ungültig ist oder keine Prüfsumme vorhanden ist, erscheint eine Warnmeldung.

7.6.2 Dateien mit Prüfsummen exportieren

Tab. 7-6: Dateien, die nach dem Export aus epBlue GxP eine Prüfsumme besitzen

Dateiformat	Datei
.export	• Applikation • Labware
.csv	• ID-Liste
.xml	• ID-Liste

▸ Dateien exportieren, wie in der Software-Bedienungsanleitung beschrieben.

7.6.3 Prüfsummen in externer Software kontrollieren

Um eine Prüfsumme aus epBlue GxP zu prüfen, gehen Sie folgendermaßen vor:

1. Prüfsumme speichern.
2. In der importierten Datei, die Zeile löschen, die die Prüfsumme enthält.
3. Zeilenumbrüche in der Datei löschen.
4. Prüfsumme für die Datei mit dem Algorithmus **SHA256** berechnen.
   Der Algorithmus ist im Microsoft .NET Framework enthalten.
5. Berechnete Prüfsumme mit der gespeicherten Prüfsumme vergleichen.

7.6.4 Prüfsummen in externer Software erstellen

Damit epBlue GxP die Prüfsummen beim Import kontrollieren kann, müssen die Prüfsummen folgendermaßen erzeugt werden.

1. Um die Prüfsumme zu berechnen, Zeilenumbrüche entfernen.
2. Prüfsumme mit dem Algorithmus SHA256 berechnen.
   Dieser Algorithmus ist im Microsoft .NET Framework enthalten.
3. Prüfsumme in die Datei eintragen.

Tab. 7-7: Prüfsummen bei bestimmten Dateiformaten

CSV-Datei	In Zeile 5, Spalte 1 = *Checksum*, Spalte 2 = berechnete Prüfsumme
XML-Datei	In Tag <Checksum> unter <ID_List>

```
ListID,,,
ListName,Methode_1_Tube_1_2,,
ListType,Input,,
CreationDate,9/20/2010 3:35 PM,,
Checksum,9799dd7c06749b192dd7fca50d5fc3acb8589218cb1246c9c16b897920a51500,,
,,,
Position,ID_1,ID_2,Name
1,1000,,
8,8000,,
```

Abb. 7-22: ID-Liste im Format csv mit Prüfsumme

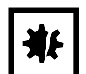
```xml
<?xml version="1.0" encoding="utf-8"?>
<ID_List>
   <ListID />
   <ListName>Method_1_Tube_1_2</ListName>
   <ListType>Input</ListType>
   <CreationDate>9/20/2010 3:37 PM</CreationDate>

<Checksum>707d9a3149fb10bbdaec1ae3330d65fe8fca6adc364d2ee5f77f94a8d5363be5</Checksum>
   <Positions>
      <PositionData>
         <Position>1</Position>
         <ID_1>1000</ID_1>
         <ID_2 />
         <Name />
      </PositionData>
      <PositionData>
         <Position>8</Position>
         <ID_1>8000</ID_1>
         <ID_2 />
         <Name />
      </PositionData>
   </Positions>
</ID_List>
```

Abb. 7-23: ID-Liste im Format xml mit Prüfsumme

8 Administration

epBlue GxP kann nur von einem Anwender der Benutzergruppe *Administrator* verwaltet werden.



ACHTUNG! Datenverlust durch verlorenes Passwort für Benutzerkonto der Benutzergruppe *Administrator*.
Wenn Sie das Passwort für das Benutzerkonto der Benutzergruppe *Administrator* nicht mehr besitzen, muss das System neu installiert werden.

- Installieren Sie mindestens zwei Benutzerkonten der Benutzergruppe *Administrator*.

8.1 Erweiterte Benutzerverwaltung

8.1.1 Sicherheit von Benutzerkonten einstellen

Voraussetzung

- Sie sind als Administrator angemeldet.

1. In epBlue GxP den Bereich *Settings* öffnen.
2. Registerkarte *Account Management* öffnen.
3. In der Spalte *Navigation* auf den Eintrag *Account Settings* klicken.

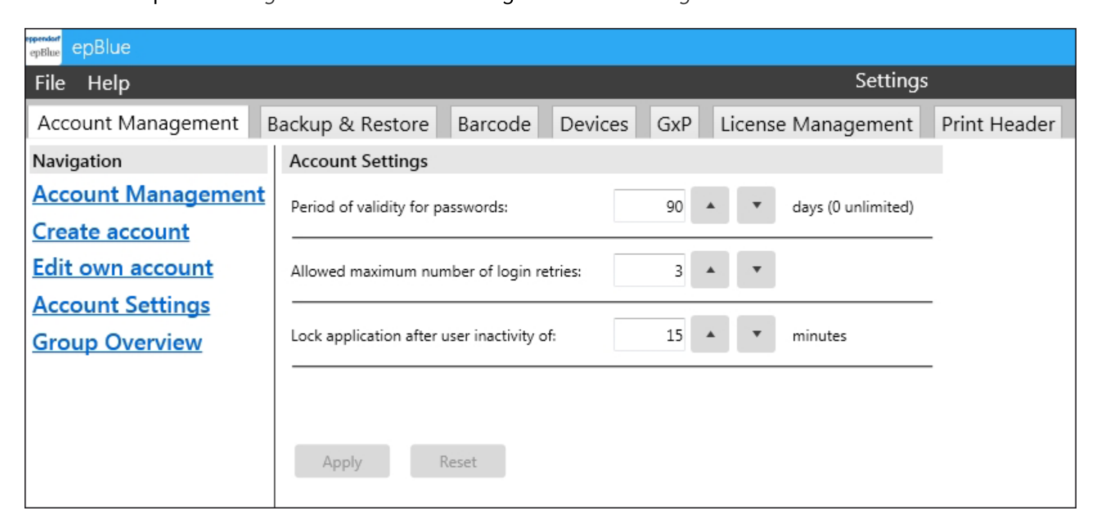


Abb. 8-1: Sicherheitseinstellungen für Benutzerkonten

Period of validity for passwords
Gültigkeit der Passwörter in Tagen.
Passwort nach Ablauf der Gültigkeit ändern.
Wenn Sie den Wert eingeben, sind die Passwörter unbegrenzt gültig.

Allowed maximum number of login retries
Zahl der fehlgeschlagenen Anmeldungen.
Wenn die Zahl der fehlgeschlagenen Anmeldungen überschritten wird, sperrt epBlue GxP das Benutzerkonto.
Benutzerkonten der Benutzergruppe *Administrator* werden nicht gesperrt.

Lock application after user inactivity
Dauer in Minuten festlegen, nach der epBlue GxP gesperrt wird.
Wenn in der definierten Zeit keine Eingaben gemacht werden, wird epBlue GxP gesperrt.

4. Um die Einstellungen zu übernehmen, auf den Button *Apply* klicken.
5. Um die Einstellungen zu verwerfen, auf den Button *Reset* klicken.
   Das Fenster *Please enter reason* erscheint.
6. Begründung für die Änderung eintragen.
   Die Begründung erscheint im Audit Trail.

Wie Sie Benutzerkonten einrichten, entnehmen sie der Software-Bedienungsanleitung.

8.1.2 Autorisierungsschema konfigurieren

Legen Sie fest, wie viele Signaturen Applikationen und Protokolle benötigen, um den Status *authorized* zu erhalten.

Voraussetzung
- Sie sind als Administrator angemeldet.

1. Auf den Bereich *Settings* klicken.
2. Registerkarte *GxP* öffnen.
3. In der Spalte *Navigation* auf das Feld *Signatures* drücken.

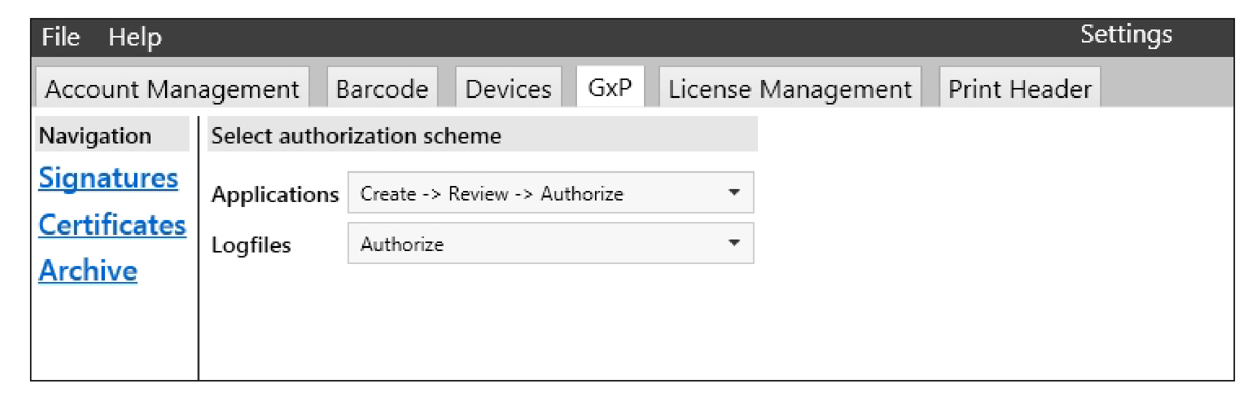


Abb. 8-2: Autorisierungsschema konfigurieren

4. Im Dropdownmenü *Applications* das Autorisierungsschema für Applikationen wählen.
5. Im Dropdownmenü *Logfiles* das Autorisierungsschema für Protokolle wählen.

Tab. 8-1: Autorisierungschema

Autorisierungsschema	**Endgültiger Status des Dokuments**	**Zahl der Signaturen**	**Zahl der Anwender**
Create -> Review -> Authorize	*authorized*	je eine Signatur der Bedeutung *created*, *reviewed* und *authorized*	3 verschiedene Anwender
Create > Authorize	*authorized*	je eine Signatur der Bedeutung *created* und *authorized*	2 verschiedene Anwender
Authorize	*authorized*	eine Signatur der Bedeutung *authorized*	1 Anwender

6. Um die Einstellungen zu löschen, auf den Button *Reset* klicken.
7. Um die Einstellungen zu übernehmen, auf den Button *Apply* klicken.
   Wenn Sie die Einstellungen übernehmen, öffnet sich das Fenster *Please enter reason*.
8. Begründung eingeben. Mit dem Button *OK* bestätigen.
   Die Begründung erscheint im Audit Trail.

8.1.3 Signaturberechtigungen festlegen

Jede Benutzergruppe besitzt definierte Rechte zum Signieren von Dateien.

Benutzergruppe	**Signieren von Applikationen**	**Signieren von Protokollen**	**Signieren von PDF-Dokumenten**
Guest	–	–	–
User Level 1	• created	• created	–
User Level 2	• created • reviewed	• created • reviewed	–
Administrator Lab	• created • reviewed • authorized	• created • reviewed • authorized	• Archive • exportierte PDF-Dokumente von Applikationen und Protokollen • IQ
Administrator	–	–	Archive

- Um die Signaturberechtigungen anzuzeigen, auf den Bereich *Account Management* klicken.
- In der Registerkarte *Account Management* auf das Feld *Group Overview* klicken.

8.1.4 Benutzerkonto entsperren

In folgenden Situationen sperrt epBlue GxP das Benutzerkonto:
- Der Anwender gibt beim Anmelden in epBlue GxP sein Passwort mehrfach falsch ein.

In folgenden Situationen sperrt epBlue GxP das Benutzerkonto nicht:
- Der Anwender gibt beim Entsperren von epBlue GxP sein Passwort mehrfach falsch ein.
- Das Benutzerkonto der Benutzergruppe *Administrator* wird nie gesperrt.

Gehen Sie wie folgt vor, um Benutzerkonten zu entsperren.

Voraussetzung
- Sie sind als Administrator angemeldet.

1. Bereich *Settings* öffnen.
2. In der Registerkarte *Account Management* auf das Feld *Account Management* klicken.
3. Im Bereich *Users* das gesperrte Benutzerkonto markieren.

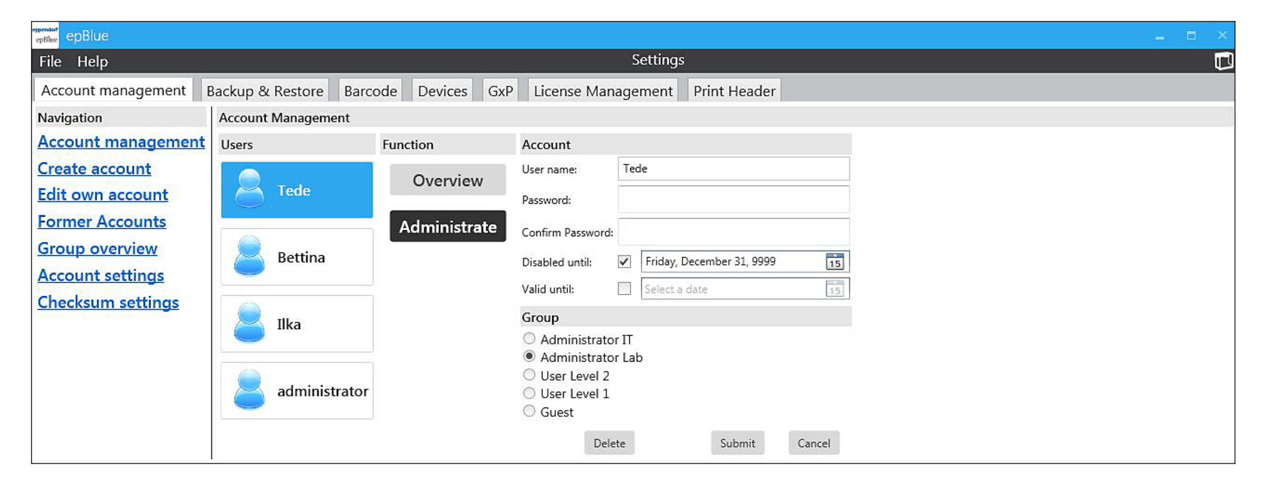


Abb. 8-3: Benutzerkonto entsperren

4. Auf das Feld *Administrate* klicken.
5. Neues Passwort für das Benutzerkonto eingeben.
6. Auf den Button *Submit* klicken.

Das Benutzerkonto ist entsperrt. Der Anwender kann sich mit dem neuen Passwort anmelden.

8.1.5 Benutzerkonto löschen

Nachdem Sie ein Benutzerkonto gelöscht haben, können Sie kein neues Benutzerkonto mit dem gleichen Namen anlegen. So stellt das System sicher, dass Namen der Anwender eindeutig sind.

Wenn Sie ein Benutzerkonto gelöscht haben, sind Signaturen des gelöschten Anwenders weiterhin gültig. Das digitale Zertifikat des gelöschten Benutzerkontos kann exportiert werden.

Wenn unter einem Benutzerkonto signierte Applikationen gespeichert sind, können Sie das Benutzerkonto nicht löschen. Um das Benutzerkonto zu löschen, archivieren Sie alle signierten Applikationen des Anwenders.

Das Löschen eines Benutzerkontos wird im Audit Trail dokumentiert. Die verwendeten Benutzerkonten finden Sie unter der Registerkarte *Former Accounts*.

Gehen Sie wie folgt vor, um Benutzerkonten zu löschen.

Voraussetzung

- Sie sind als Administrator angemeldet.
- Unter dem zu löschenden Benutzerkonto sind keine signierten Applikationen gespeichert.

1. Bereich *Settings* öffnen.
2. In der Registerkarte *Account Management* auf das Feld *Account Management* klicken.
3. Im Bereich *Users* das zu löschende Benutzerkonto wählen.
4. Button *Administrate* klicken.
5. Um das Löschen des Benutzerkontos zu bestätigen, auf den Button *Remove* klicken.
6. Begründung für das Löschen eingeben. Mit dem Button *OK* bestätigen.
   Die Begründung erscheint im Audit Trail.

8.2 Kontrolle der Prüfsumme aktivieren

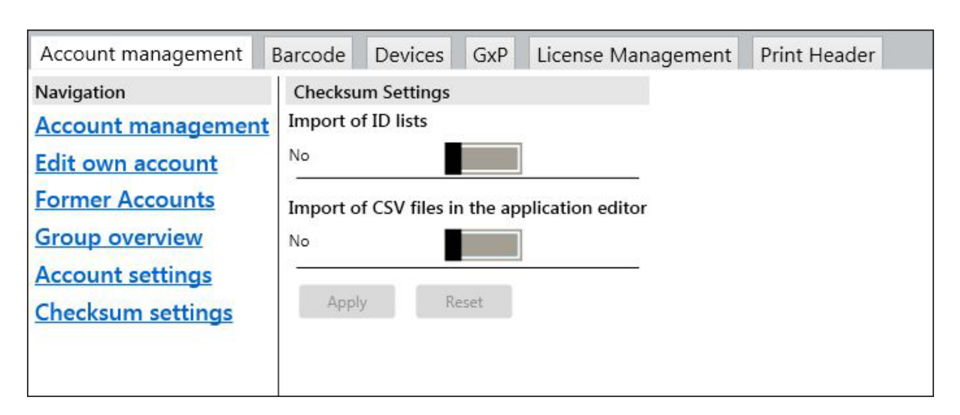


Abb. 8-4: Kontrolle der Prüfsumme aktivieren

Import of ID lists
Prüfsumme beim Importieren von ID-Listen prüfen oder nicht prüfen.

Import of CSV files in the application editor
Prüfsumme beim Importieren von CSV-Dateien prüfen oder nicht prüfen.

Um die Kontrolle der Prüfsumme zu aktivieren und deaktivieren, gehen Sie wie folgt vor.

Voraussetzung

- Sie sind als *Administrator* oder *Administrator Lab* angemeldet.

1. In epBlue GxP den Bereich *Settings* öffnen.
2. Registerkarte *Account Management* wählen.
3. In der Spalte *Navigation* den Eintrag *Checksum settings* wählen.
4. Einstellungen für die Prüfung der Prüfsumme wählen.

8.3 Daten archivieren

Sie können Daten als signierte PDF-Dokumente archivieren. Die Daten werden beim Archivieren aus der epBlue-Datenbank entfernt.

Sie können folgende Daten archivieren:
- Applikationen mit dazu gehörenden Protokollen
- Einzelne Protokolle
- Teile des Audit Trail

Archivierte PDF-Dokumente können mit digitalen Signaturen geprüft werden. Um die digitalen Signaturen zu prüfen, exportieren Sie die Zertifikate aus epBlue GxP. Bewahren Sie die Zertifikate zusammen mit den archivierten Daten auf.

Sie können archivierte PDF-Dokumente drucken.



ACHTUNG! Löschen von Daten aus der Datenbank beim Archivieren.
Wenn Sie Daten archivieren, exportiert epBlue die Daten als PDF-Dokumente. Die Daten werden aus der epBlue-Datenbank entfernt. Archivierten Daten können nicht wieder in die epBlue-Datenbank importiert werden.

- Archivieren Sie keine Daten, die Sie noch benötigen.

8.3.1 Applikationen und Protokolle archivieren

Sie können folgende Daten nicht archivieren:
- Geöffnete Applikationen mit dazu gehörenden Protokollen
- Benutzerkonto des angemeldeten Anwenders

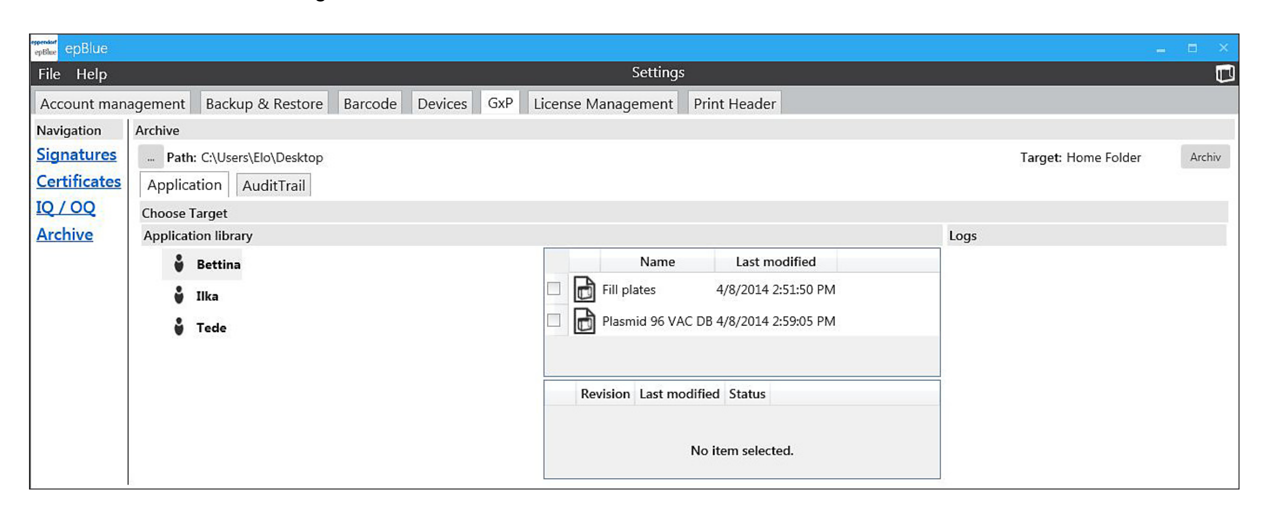


Abb. 8-5: Fenster *Archive*

Voraussetzung
- Sie sind als *Administrator* oder *Administrator Lab* angemeldet.

1. In epBlue GxP den Bereich *Settings* öffnen.
2. Registerkarte *GxP* wählen.
3. In der Spalte *Navigation* auf den Eintrag *Archive* klicken.
4. Ordner wählen, in den die Dateien archiviert werden sollen.
5. Dateien wählen, die archiviert werden sollen.

   Um mehrere Dateien zu wählen, die Tasten **CTRL** oder die **Umschalt** drücken. Gleichzeitig die Dateien mit der Maus markieren.

Tab. 8-2: Dateien für die Archivierung wählen

Alle Applikationen und Protokolle eines Anwenders	Alle Applikationen und Protokolle in dem Verzeichnis eines Anwenders	Alle Revisionen und Protokolle einer Applikation	Protokolle einer Revision
▶ Name des Anwenders im Bereich *Applikation Library* wählen.	▶ In der *Applikation Library* im Ordner des Anwenders den Namen des Verzeichnisses wählen.	▶ Name der Applikation wählen.	1. Nummer der Revision im Bereich *Revision* wählen. 2. Protokolle in Bereich *Logfiles* wählen.

3. Auf den Button *Archive* klicken.

   Das Fenster *Information* erscheint.

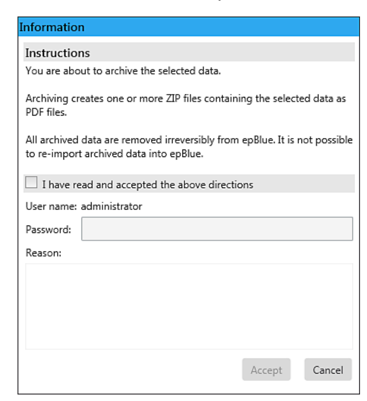


Abb. 8-6: Fenster *Information*

4. Um die markierten Daten zu archivieren, Checkbox *I have read and accepted the above directions* aktivieren.
5. Passwort eingeben.
6. Optional im Feld *Reason* eine Begründung für die Archivierung eingeben.

   Die Begründung erscheint im Audit Trail und im Zertifikat der PDF-Dokumente.

7. Auf den Button *Accept* klicken.

   Die Daten werden als signierte PDF-Dokumente in einem ZIP-Archiv gespeichert. Nach der Archivierung werden die Daten aus der epBlue-Datenbank gelöscht.

8.3.2 Audit Trail archivieren

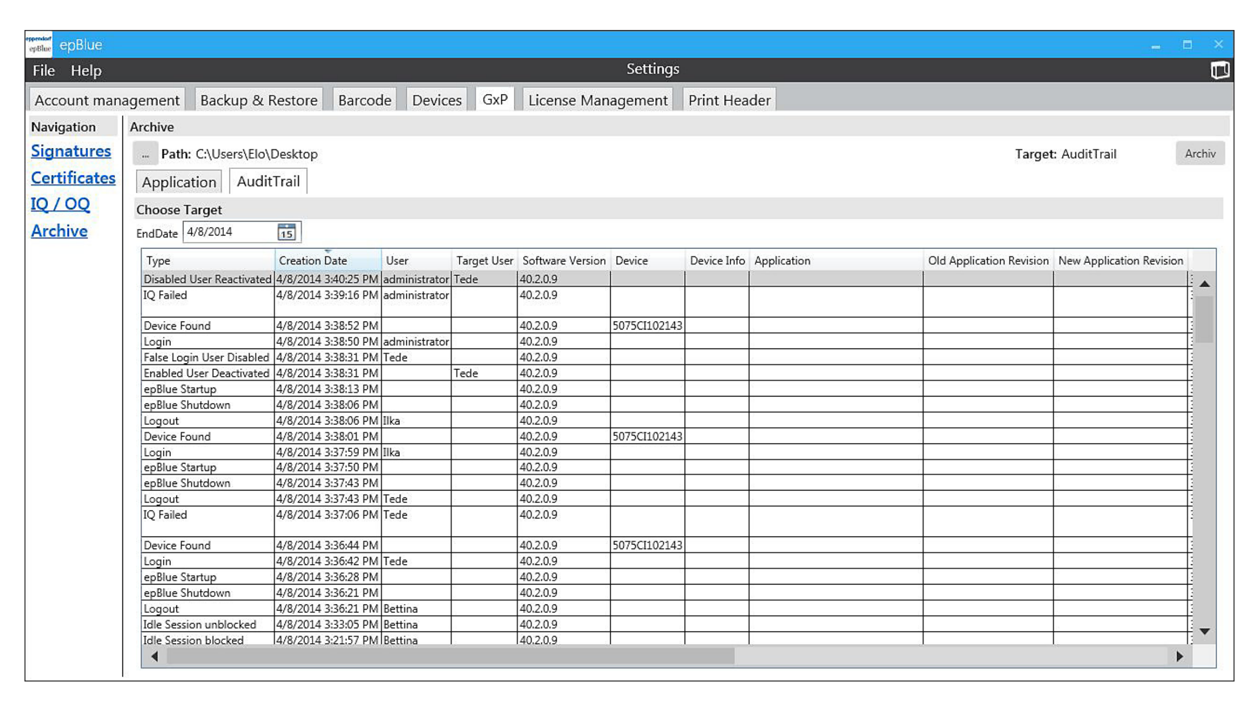


Abb. 8-7: Auswahl zur Archivierung des Audit Trail

Voraussetzung

- Sie sind als *Administrator* oder *Administrator Lab* angemeldet.

1. In epBlue GxP den Bereich *Settings* öffnen.
2. Registerkarte *GxP* wählen.
3. In der Spalte *Navigation* auf den Eintrag *Archive* klicken.
4. Registerkarte *Audit Trail* öffnen.
5. Ordner wählen, in den die Dateien archiviert werden sollen.
6. Im Feld *End Date* festlegen, bis zu welchem Datum die Einträge im Audit Trail archiviert werden sollen.
   epBlue GxP zeigt, welche Einträge archiviert werden.
7. Auf den Button *Archive* klicken.
   Das Fenster *Information* öffnet sich.
8. Checkbox *I have read and accepted the above directions* aktivieren.
9. Passwort eingeben.
10. Optional Begründung für die Archivierung eingeben.
    Die Begründung erscheint im Audit Trail und im Zertifikat des PDF-Dokuments.
11. Auf den Button *Accept* klicken.
    Die Daten werden als signierte PDF-Dokumente gespeichert. Nach der Archivierung werden die Daten aus der epBlue-Datenbank gelöscht.

8.4 Systemkonfiguration prüfen

Bei der Installation erstellt der autorisierten Service eine Referenzliste (IQ Reference). Die Referenzliste enthält die Konfiguration relevanter Komponenten von Software und Hardware. Die Referenzliste wird im System gespeichert.

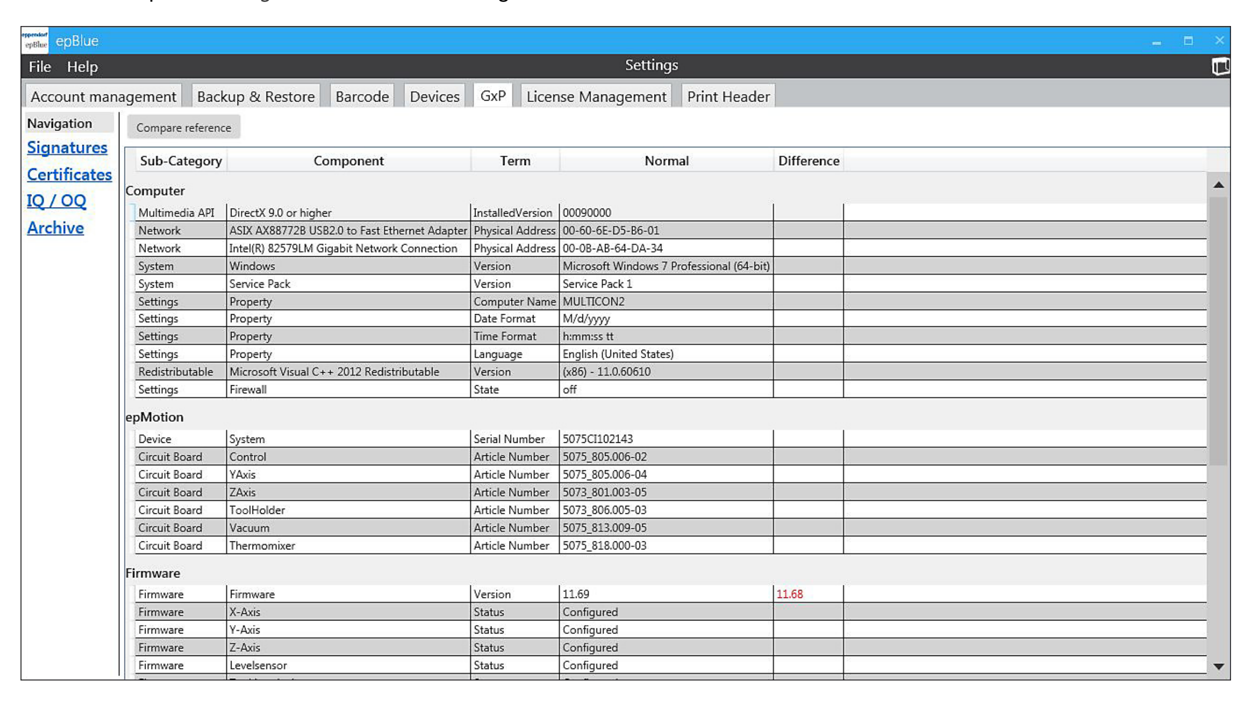
Sie können die aktuelle Konfiguration mit der Referenzliste vergleichen. Damit prüfen Sie, welche Komponenten verändert wurden.

Gehen Sie folgendermaßen vor:

Voraussetzung

- Sie sind als *Administrator* oder *Administrator Lab* angemeldet.

1. In epBlue GxP den Bereich *Settings* öffnen.
2. Registerkarte *GxP* wählen.
3. In der Spalte *Navigation* auf den Eintrag *IQ/OQ* klicken.



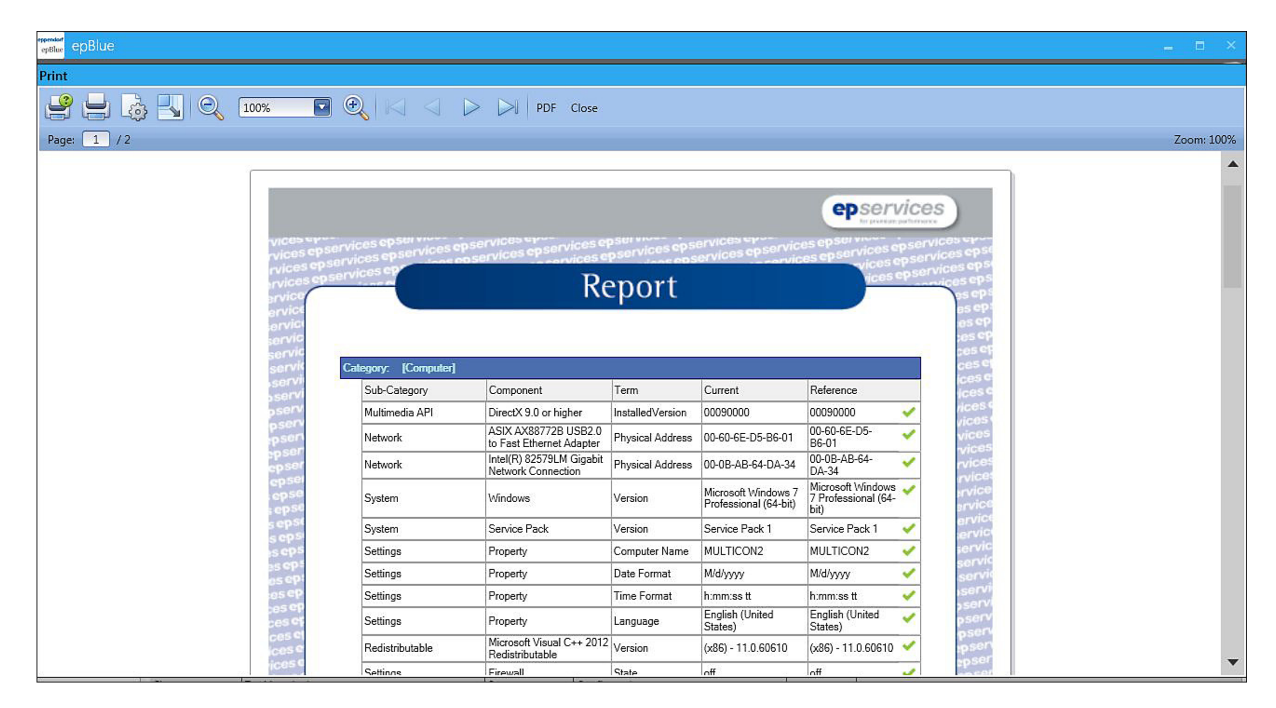
Sub-Category	Component	Term	Normal	Difference
Computer				
Multimedia API	DirectX 9.0 or higher	InstalledVersion	00090000	
Network	ASIX AX88772B USB2.0 to Fast Ethernet Adapter	Physical Address	00-60-6E-D5-B6-01	
Network	Intel(R) 82579LM Gigabit Network Connection	Physical Address	00-0B-AB-64-DA-34	
System	Windows	Version	Microsoft Windows 7 Professional (64-bit)	
System	Service Pack	Version	Service Pack 1	
Settings	Property	Computer Name	MULTICON2	
Settings	Property	Date Format	M/d/yyyy	
Settings	Property	Time Format	h:mm:ss tt	
Settings	Property	Language	English (United States)	
Redistributable	Microsoft Visual C++ 2012 Redistributable	Version	(x86) - 11.0.60610	
Settings	Firewall	State	off	
epMotion				
Device	System	Serial Number	5075CI102143	
Circuit Board	Control	Article Number	5075_805.006-02	
Circuit Board	YAxis	Article Number	5075_805.006-04	
Circuit Board	ZAxis	Article Number	5073_801.003-05	
Circuit Board	ToolHolder	Article Number	5073_806.005-03	
Circuit Board	Vacuum	Article Number	5075_813.009-05	
Circuit Board	Thermomixer	Article Number	5075_818.000-03	
Firmware				
Firmware	Firmware	Version	11.69	11.68
Firmware	X-Axis	Status	Configured	
Firmware	Y-Axis	Status	Configured	
Firmware	Z-Axis	Status	Configured	
Firmware	Levelsensor	Status	Configured	

Abb. 8-8: Systemkonfiguration prüfen

4. Auf den Button *Compare reference* klicken.

   Das System ermittelt die aktuelle Konfiguration relevanter Komponenten von Software und Hardware und vergleicht sie mit der Referenzliste.
   Der Prüfbericht erscheint im Fenster *Preview*.

5. Prüfbericht ggf. drucken oder als PDF-Dokument speichern.
6. Fenster *Preview* schließen.



Sub-Category	Component	Term	Current	Reference
Multimedia API	DirectX 9.0 or higher	InstalledVersion	00090000	00090000
Network	ASIX AX88772B USB2.0 to Fast Ethernet Adapter	Physical Address	00-60-6E-D5-B6-01	00-60-6E-D5-B6-01
Network	Intel(R) 82579LM Gigabit Network Connection	Physical Address	00-0B-AB-64-DA-34	00-0B-AB-64-DA-34
System	Windows	Version	Microsoft Windows 7 Professional (64-bit)	Microsoft Windows 7 Professional (64-bit)
System	Service Pack	Version	Service Pack 1	Service Pack 1
Settings	Property	Computer Name	MULTICON2	MULTICON2
Settings	Property	Date Format	M/d/yyyy	M/d/yyyy
Settings	Property	Time Format	h:mm:ss tt	h:mm:ss tt
Settings	Property	Language	English (United States)	English (United States)
Redistributable	Microsoft Visual C++ 2012 Redistributable	Version	(x86) - 11.0.60610	(x86) - 11.0.60610
Settings	Firewall	State	off	off

Abb. 8-9: Prüfbericht

Kategorie	**Beschreibung**
Firmware	Firmware-Version der Baugruppen des Geräts.
PC-Software	Versionen von Komponenten von epBlue GxP.
Industrial Computer	Versionen von Komponenten anderer Hersteller, die in epBlue GxP verwendet werden. Konfiguration von Komponenten des Betriebssystems.
epMotion	Versionen von Komponenten der epMotion 5075. Seriennummer der epMotion 5075.

Der Prüfbericht enthält 5 Kategorien. Die Spalte *Term* zeigt, welches Kriterium einer Komponente verglichen wurde.

Abweichungen zwischen der aktuellen Konfiguration und der Referenzliste werden in roter Schrift dargestellt. Abweichungen sind im Ausdruck und im PDF-Dokument mit einem roten Kreuz markiert.

9 Problembehebung

9.1 Allgemeine Fehler

Weitere Anweisungen zur Problembehebung finden Sie in Software-Bedienungsanleitung und Hardware-Bedienungsanleitung.

Symptom/Meldung	Mögliche Ursache	Abhilfe
No valid reference file has been found. Please contact Eppendorf Service.	• Die Referenzliste für die Funktion *Compare Reference* ist nicht erzeugt worden. • Die Referenzliste für die Funktion *Compare Reference* ist nicht lesbar. • Die Referenzliste für die Funktion *Compare Reference* ist nicht gültig.	▸ Um eine neue Referenzliste erstellen zu lassen, wenden Sie sich an den autorisierten Service.
Die Signatur des PDF-Dokuments kann nicht verifiziert werden.	• Das Master-Zertifikat wurde nicht in das PDF-Anzeigeprogramm importiert.	▸ Master-Zertifikat in das PDF-Anzeigeprogramm importieren.
	• Das PDF-Anzeigeprogramm vertraut dem Master-Zertifikat nicht.	▸ Master-Zertifikat als vertrauenswürdig einstufen.
Ein Protokoll kann nicht signiert werden.	• Eine Revision des Protokolls besitzt nicht den Status *authorized*.	1. Revision mit dem Status *authorized* signieren. 2. Applikation neu starten.
Ein Protokoll oder einer Applikation kann nicht signiert werden.	• Der Anwender besitzt nicht das Recht, die Signatur zu vergeben.	▸ Signaturberechtigungen für Protokolle oder Applikationen ändern. ▸ Den Anwender einer anderen Benutzergruppe zuweisen.
Eine Applikation kann nicht gelöscht werden.	• Mindestens eine Revision der Applikation ist signiert.	1. Applikation archivieren. 2. Applikation löschen.
Ein Benutzerkonto kann nicht gelöscht werden.	• Unter dem Benutzerkonto ist mindestens eine signierte Applikation gespeichert.	1. Signierte Applikationen archivieren, die unter dem Benutzerkonto gespeichert sind. 2. Benutzerkonto löschen.
Wenn eine Applikation gestartet wird, kann die Einstellung *Levels* des optischen Sensors nicht verändert werden.	• Die gestartete Revision ist signiert.	▸ Als Anwender der Benutzergruppe *Administrator* die Einstellungen des optischen Sensors ändern.

10 Bestellinformationen

10.1 Software

Best.-Nr. (International)	Beschreibung
5075 002.728	**epBlue GxP** Umrüstsatz für epMotion mit MultiCon mit Seriennummer > 4000 mit Dokumentationsordner
5075 002.701	**epBlue ID** Umrüstsatz für epMotion mit MultiCon mit Seriennummer > 4000 mit Barcode-Reader

Index



Evaluate your manual

Give us your feedback.
www.eppendorf.com/manualfeedback

Your local distributor: www.eppendorf.com/contact
Eppendorf AG · 22331 Hamburg · Germany
eppendorf@eppendorf.com · www.eppendorf.com